

ESSEX PRIMARY SCHOOL

Online Safety Policy

Reviewed September 2016

Next Review due September 2017

This policy is part of the School's Statutory Safeguarding Policy. Any issues and concerns with online safety must follow the school's safeguarding and child protection processes.

Contents

1. Introduction and Overview

- Rationale and Scope
- Roles and responsibilities
- How the policy is communicated to staff/pupils/community
- Handling complaints
- Reviewing and Monitoring

2. Education and Curriculum

- Pupil online safety curriculum
- Staff and governor training
- Parent awareness and training

3. Expected Conduct and Incident Management

4. Managing the IT Infrastructure

- Internet access, security (virus protection) and filtering
- Network management (user access, backup, curriculum and admin)
- Passwords policy
- E-mail
- School website
- Learning platform
- Social networking
- Video Conferencing

5. Data Security

- Management Information System access
- Data transfer
- Asset Disposal

6. Equipment and Digital Content

- Personal mobile phones and devices
- Digital images and video

Appendices:

- A1: Acceptable Use Agreement (Staff, Volunteers and Governors)
- A2: Acceptable Use Agreements (Pupils – adapted for phase)
- A3: Acceptable Use Agreement including photo/video permission (Parents)
- A4: Protocol for responding to online safety incidents- handling infringements
Digitally Confident Guidelines
- A5: Prevent Guidance
- A6: Data security
- A7: Search and Confiscation guidance from DfE

1. Introduction and Overview

Rationale

The purpose of this policy is to:

- Set out the key principles expected of all members of the school community at Essex Primary School with respect to the use of IT-based technologies.
- Safeguard and protect the children and staff.
- Assist school staff working with children to work safely and responsibly with the Internet and other IT and communication technologies and to monitor their own standards and practice.
- Set clear expectations of behaviour and/or codes of practice relevant to responsible use of the Internet for educational, personal or recreational use for the whole school community.
- Have clear structures to deal with online abuse such as online bullying
- Ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- Minimise the risk of misplaced or malicious allegations made against adults who work with students.

The main areas of risk for our school community can be summarised as follows:

Content

- Exposure to inappropriate content
- Lifestyle websites promoting harmful behaviours
- Hate content
- Content validation: how to check authenticity and accuracy of online content

Contact

- Grooming (sexual exploitation, radicalisation etc.)
- Online bullying in all forms
- Social or commercial identity theft, including passwords

Conduct

- Aggressive behaviours (bullying)
- Privacy issues, including disclosure of personal information
- Digital footprint and online reputation
- Health and well-being (amount of time spent online, gambling, body image)
- Sexting
- Copyright (little care or consideration for intellectual property and ownership)

Scope

This policy applies to all members of Essex Primary School community (including staff, students/pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of Essex Primary IT systems, both in and out of Essex Primary.

Roles and responsibilities

Role	Key Responsibilities
Headteacher	<ul style="list-style-type: none">• Must be adequately trained in off-line and online safeguarding, in-line with statutory guidance and relevant Local Safeguarding Children Board (LSCB) guidance• To lead a 'safeguarding' culture, ensuring that online safety is fully integrated with whole school safeguarding.• To take overall responsibility for online safety provision• To take overall responsibility for data management and information security, Senior Information Risk Officer (SIRO) ensuring school's provision follows best practice in information handling• To ensure the school uses appropriate IT systems and services including, filtered Internet Service, e.g. LGfL services• To be responsible for ensuring that all staff receive suitable training to carry out their safeguarding and online safety roles• To be aware of procedures to be followed in the event of a serious online safety incident• Ensure suitable 'risk assessments' undertaken so the curriculum meets needs of pupils, including risk of children being radicalised• To receive regular monitoring reports from the Online Safety Co-ordinator• To ensure that there is a system in place to monitor and support staff who carry out internal online safety procedures, e.g. network manager• To ensure Governors are regularly updated on the nature and effectiveness of the school's arrangements for online safety• To ensure school website includes relevant information.
Online Safety Co-ordinator/Designated Child Protection Lead (This may be the same person)	<ul style="list-style-type: none">• Take day to day responsibility for online safety issues and a leading role in establishing and reviewing the school's online safety policy/documents• Promote an awareness and commitment to online safety throughout the school community• Ensure that online safety education is embedded within the curriculum

Role	Key Responsibilities
	<ul style="list-style-type: none"> • Liaise with school technical staff where appropriate • To communicate regularly with SLT and the designated online safety Governor/committee to discuss current issues, review incident logs and filtering/change control logs • To ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident • To ensure that online safety incidents are logged as a safeguarding incident • Facilitate training and advice for all staff • Oversee any pupil surveys / pupil feedback on online safety issues • Liaise with the Local Authority and relevant agencies • Is regularly updated in online safety issues and legislation, and be aware of the potential for serious child protection concerns.
Governors/Safeguarding governor (including online safety)	<ul style="list-style-type: none"> • To ensure that the school has in place policies and practices to keep the children and staff safe online • To approve the Online Safety Policy and review the effectiveness of the policy • To support the school in encouraging parents and the wider community to become engaged in online safety activities • The role of the online safety Governor will include: regular review with the online safety Co-ordinator.
Computing Curriculum Leader	<ul style="list-style-type: none"> • To oversee the delivery of the online safety element of the Computing curriculum
Network Manager/technician	<ul style="list-style-type: none"> • To report online safety related issues that come to their attention, to the Online Safety Coordinator • To manage the school's computer systems, ensuring <ul style="list-style-type: none"> - school password policy is strictly adhered to. - systems are in place for misuse detection and malicious attack (e.g. keeping virus protection up to date) - access controls/encryption exist to protect personal and sensitive information held on school-owned devices - the school's policy on web filtering is applied and updated on a regular basis • That they keep up to date with the school's online safety policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant • That the use of school technology and online platforms are regularly monitored and that any misuse/attempted misuse is reported to the online safety co-ordinator/Headteacher • To ensure appropriate backup procedures and disaster recovery

Role	Key Responsibilities
	<p>plans are in place</p> <ul style="list-style-type: none"> • To keep up-to-date documentation of the school's online security and technical procedures
<p>Data and Information (Asset Owners) Managers, Information Awareness Officers (IAOs)</p>	<ul style="list-style-type: none"> • To ensure that the data they manage is accurate and up-to-date • Ensure best practice in information management. i.e. have appropriate access controls in place, that data is used, transferred and deleted in-line with data protection requirements. • The school must be registered with Information Commissioner
<p>LGfL Nominated contact(s)</p>	<ul style="list-style-type: none"> • To ensure all LGfL services are managed on behalf of the school following data handling procedures as relevant
<p>Teachers</p>	<ul style="list-style-type: none"> • To embed online safety across the curriculum • To supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant) • To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws
<p>All staff</p>	<ul style="list-style-type: none"> • To read, understand, sign and adhere to the school staff Acceptable Use Agreement/Policy, and understand any updates annually. The AUP is signed by new staff on induction. • To report any suspected misuse or problem to the online safety coordinator • To maintain an awareness of current online safety issues and guidance e.g. through CPD • To model safe, responsible and professional behaviours in their own use of technology <p>Exit strategy</p> <ul style="list-style-type: none"> • At the end of the period of employment/volunteering to return any equipment or devices loaned by the school. This will include leaving PIN numbers, IDs and passwords to allow devices to be reset, or meeting with line manager and technician on the last day to log in and allow a factory reset.
<p>Pupils</p>	<ul style="list-style-type: none"> • Read, understand, sign and adhere to the Student/Pupil Acceptable Use Policy annually • To understand the importance of reporting abuse, misuse or access to inappropriate materials • To know what action to take if they or someone they know feels worried or vulnerable when using online technology • To understand the importance of adopting safe behaviours and

Role	Key Responsibilities
	<p>good online safety practice when using digital technologies out of school and realise that the school's online safety policy covers their actions out of school</p> <ul style="list-style-type: none"> • To contribute to any 'pupil voice' / surveys that gathers information of their online experiences
Parents/carers	<ul style="list-style-type: none"> • To read, understand and promote the school's Pupil Acceptable Use Agreement with their child/ren • to consult with the school if they have any concerns about their children's use of technology • to support the school in promoting online safety and endorse the Parents' Acceptable Use Agreement which includes the pupils' use of the Internet and the school's use of photographic and video images
External groups including Parent groups	<ul style="list-style-type: none"> • Any external individual/organisation will sign an Acceptable Use agreement prior to using technology or the Internet within school • to support the school in promoting online safety • To model safe, responsible and positive behaviours in their own use of technology.

Communication:

The policy will be communicated to staff/pupils/community in the following ways:

- Policy to be posted on the school website/ school library / curriculum network class.
- Policy to be part of school induction pack for new staff.
- Regular updates and training on online safety for all staff.
- Acceptable use agreements discussed with staff and pupils at the start of each year.
Acceptable use agreements to be issued to whole school community, on entry to the school.

Handling Incidents:

Owing to the international scale and linked nature of internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of internet access. However:

- The school will take all reasonable precautions to ensure online safety.
- Staff and pupils are given information about infringements in use and possible sanctions – see appendix 4.
- Online Safety Coordinator acts as first point of contact for any incident.
- Any suspected online risk or infringement is reported to Online Safety Coordinator that day and documented.
- Online Bullying incidences will be reported and acted upon in accordance with our Bullying Policy.
- Complaints related to Child Protection are dealt with in accordance with our Child Protection Policy.
- Any concern about staff misuse is always referred directly to the Headteacher, unless the concern is about the Headteacher in which case the complaint is referred to the Chair of Governors and the LADO (Local Authority's Designated Officer).
- Sanctions applied may include; meeting with parents / carers, removal of internet access, recording of incident in appropriate school log, referral to LA / Police.

Review and Monitoring

The online safety policy is referenced within other school policies (e.g. Safeguarding and Child Protection policy, Anti-Bullying policy, PSHE, Computing policy).

- The online safety policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the school.
- There is widespread ownership of the policy and it has been agreed by the SLT and approved by Governors. All amendments to the school online safety policy will be disseminated to all members of staff and pupils.

2. Education and Curriculum

Pupil online safety curriculum

This school:

- has a clear, progressive online safety education programme which is embedded across the curriculum. This covers a range of skills and behaviours appropriate to their age and experience, covering topics such as online bullying, sexting, online contact and communications, authenticity of online content, copyright etc (see subject leader for full details);
- plans online use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas;
- will remind students about their responsibilities through the pupil Acceptable Use Agreement(s); appendix 2
- ensures staff are aware of their responsibility to model safe and responsible behaviour in their own use of technology, e.g. use of passwords, logging-off, use of content, research skills, copyright; appendix 1
- ensures that staff and pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright/intellectual property rights; appendices 1, 2
- ensure pupils only use school-approved systems and publish within appropriately secure / age-appropriate environments.

Staff and governor training

This school:

- makes regular training available to staff on online safety issues and the school's online safety education program;
- provides as part of the induction process, all new staff [including those on university/college placement and work experience] with information and guidance on the Online Safety Policy and the school's Acceptable Use Agreements.

Parent awareness and training

This school:

- provide online safety information and guidance at initial meeting including AUP signing;
- runs a rolling programme of online safety advice, guidance and training for parents.

3. Expected Conduct and Incident management

Expected conduct

In this school, all users:

- are responsible for using the school IT and communication systems in accordance with the relevant Acceptable Use Agreements;
- understand the significance of misuse or access to inappropriate materials and are aware of the consequences;
- understand it is essential to report abuse, misuse or access to inappropriate materials and know how to do so;
- understand the importance of adopting good online safety practice when using digital technologies in and out of school;
- know and understand school policies on the use of mobile and hand held devices including cameras.

Staff, volunteers and contractors

- know to be vigilant in the supervision of children at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas where older pupils have more flexible access;
- know to take professional, reasonable precautions when working with pupils, previewing websites before use; using age-appropriate (pupil friendly) search engines where more open Internet searching is required with younger pupils.

Parents/Carers

- should provide consent for pupils to use the Internet, as well as other technologies, as part of the online safety acceptable use agreement form;
- should know and understand what the school's rules of appropriate use for the whole school community are and what sanctions result from misuse.

Incident Management

In this school:

- there is strict monitoring and application of the online safety policy and a differentiated and appropriate range of sanctions;
- all members of the school are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the school's escalation processes;
- support is actively sought from other agencies as needed (i.e. the local authority, NPW, LGfL, UK Safer Internet Centre helpline, Child Exploitation and Online Protection Centre (CEOP), Prevent Officer, Police, Internet Watch Foundation (IWF) in dealing with online safety issues;
- monitoring and reporting of online safety incidents takes place and contribute to developments in policy and practice in online safety within the school;
- parents/carers are specifically informed of online safety incidents involving young people for whom they are responsible;

- the Police will be contacted if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law;
- we will immediately refer any suspected illegal material to the appropriate authorities – Police, Internet Watch Foundation and inform the LA.

4. Managing IT and Communication System

Internet access, security (virus protection) and filtering

This school:

- Informs all users that Internet/email use is monitored.
- Has the educational filtered secure broadband connectivity through the LGfL.
- Uses the LGfL filtering system which blocks sites that fall into categories (e.g. adult content, race hate, gaming). All changes to the filtering policy are logged and only available to staff with the approved 'web filtering management' status.
- Uses USO user-level filtering where relevant.
- Ensures network health through use of Sophos anti-virus software (from LGfL).
- Uses DfE, LA or LGfL approved systems including DfE S2S, LGfL USO FX2, Egress secure file/email to send 'protect-level' (sensitive personal) data over the Internet.
- Uses encrypted devices or secure remote access where staff need to access 'protect-level' (sensitive personal) data off-site.
- Works in partnership with the LGfL to ensure any concerns about the system are communicated so that systems remain robust and protect students.

Network management (user access, backup)

This school

- Uses individual, audited log-ins for all users - the LGfL USO system.
- Uses guest accounts occasionally for external or short term visitors for temporary access to appropriate services.
- Ensures the Systems Administrator/network manager is up-to-date with LGfL services and policies/requires the Technical Support Provider to be up-to-date with LGfL services and policies.
- Has daily back-up of school data (admin and curriculum).
- Uses secure, 'Cloud' storage for data back-up that conforms to DfE guidance.
- Storage of all data within the school will conform to the EU and UK data protection requirements; Storage of data online, will conform to the EU data protection directive where storage is hosted within the EU.

To ensure the network is used safely, this school:

- Ensures staff read and sign that they have understood the school's online safety Policy. Following this, they are set-up with Internet, email access and network access. Online access to service is through a unique, audited username and password. We also provide a different username and password for access to our school's network.
- All pupils have their own unique username and password which gives them access to the Internet and other services.
- Makes clear that no one should log on as another user and makes clear that pupils should never be allowed to log-on or use teacher and staff logins.

- Has set-up the network with a shared work area for pupils and one for staff. Staff and pupils are shown how to save work and access work from these areas.
- Requires all users to log off / or lock screens when they have finished working or are leaving the computer unattended.
- Ensures all equipment owned by the school and/or connected to the network has up to date virus protection.
- Makes clear that staff are responsible for ensuring that any computer or laptop loaned to them by the school, is used only to support their professional responsibilities.
- Makes clear that staff accessing LA systems do so in accordance with any Corporate policies; e.g. Borough email or Intranet; finance system, Personnel system etc.
- Maintains equipment to ensure Health and Safety is followed.
- Does not allow any outside Agencies to access our network remotely except where there is a clear professional need and then access is audited restricted and is only through approved systems.
- Has a clear disaster recovery system in place that includes a secure, remote off site back up of data.
- This school uses secure data transfer; this includes DfE secure S2S website for all CTF files sent to other schools.
- Ensures that all pupil level data or personal data sent over the Internet is encrypted.
- Our wireless network has been secured to industry standard Enterprise security level /appropriate standards suitable for educational use.
- All IT and communications systems installed professionally and regularly reviewed to ensure they meet health and safety standards.

Password policy

- This school makes it clear that staff and pupils must always keep their passwords private, must not share with others; If a password is compromised the school should be notified immediately.
- All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password(s) private.
- We require staff to use STRONG passwords.
- We require staff to change their passwords into the MIS, LGfL USO admin site, every 90 days/twice a year.
- We require staff using critical systems to use two factor authentication.

E-mail

This school

- Provides staff with an email account for their professional use, LGfL email and makes clear personal email should be through a separate account.
- We use anonymous or group e-mail addresses, for example info@schoolname.la.sch.uk/head@schoolname.la.sch.uk/or class e-mail addresses.

- Will contact the Police if one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law.
- Will ensure that email accounts are maintained and up to date.
- We use a number of LGfL-provided technologies to help protect users and systems in the school, including desktop anti-virus product Sophos, plus direct email filtering for viruses.

Pupils:

- We use LGfL pupil email system which are intentionally 'anonymised' for pupil protection.
- Pupils are taught about the online safety and 'netiquette' of using e-mail both in school and at home.

Staff:

- Staff will use LA or LGfL e-mail systems for professional purposes.
- Access in school to external personal e mail accounts may be blocked.
- Never use email to transfer staff or pupil personal data. 'Protect-level' data should never be transferred by email. If there is no secure file transfer solution available for the situation, then the data / file must be protected with security encryption.

School website

- The Headteacher, supported by the Governing body, takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained.
- The school web site complies with statutory DFE requirements.
- Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status.
- Photographs published on the web do not have full names attached. We do not use pupils' names when saving images in the file names or in the tags when publishing to the school website.

Cloud Environments

- Uploading of information on the schools' online learning space is shared between different staff members according to their responsibilities e.g. all class teachers upload information in their class areas.
- Photographs and videos uploaded to the school's online environment will only be accessible by members of the school community.
- In school, pupils are only able to upload and publish within school approved 'Cloud' systems.

Social networking

Staff, Volunteers and Contractors

- Staff are instructed to always keep professional and private communication separate.
- Teachers are instructed not to run social network spaces for student use on a personal basis or to open up their own spaces to their students, but to use the schools' preferred system for such communications.

School staff will ensure that in private use:

- No reference should be made in social media to students/pupils, parents/carers or school staff.
- School staff should not be online friends with any pupil/student. Any exceptions must be approved by the Headteacher.
- They do not engage in online discussion on personal matters relating to members of the school community.
- Personal opinions should not be attributed to the school /academy or local authority and personal opinions must not compromise the professional role of the staff member, nor bring the school into disrepute.
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Pupils:

- Are taught about social networking, acceptable behaviours and how to report misuse, intimidation or abuse through our online safety curriculum work.
- Students are required to sign and follow our [age appropriate] pupil Acceptable Use Agreement appendix 2.

Parents:

- Parents are reminded about social networking risks and protocols through our parental Acceptable Use Agreement appendix 3, Parents and Carers Online Safety Workshops, and additional communications materials when required.
- Are reminded that they need to ask permission before uploading photographs, videos or any other information about other people.

CCTV

- We have CCTV in the school as part of our site surveillance for staff and student safety. The use of CCTV is clearly signposted in the school. We will not reveal any recordings without appropriate permission.

5. Data security: Management Information System access and Data transfer

Strategic and operational practices

At this school:

- The Head Teacher is the Senior Information Risk Officer (SIRO).
- Staff are clear who are the key contact(s) for key school information (the Information Asset Owners) are. We have listed the information and information asset owners.
- We ensure staff know who to report any incidents where data protection may have been compromised.
- All staff are DBS checked and records are held in a single central record.

Technical Solutions

- Staff have secure area(s) on the network to store sensitive files.
- We require staff to log-out of systems when leaving their computer, but also enforce lock-out after idle time.
- We use the LGfL USO AutoUpdate, for creation of online user accounts for access to broadband services and the LGfL content.
- All servers are in lockable locations and managed by DBS-checked staff.
- Details of all school-owned hardware will be recorded in a hardware inventory.
- Details of all school-owned software will be recorded in a software inventory.
- Disposal of any equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2006 and/or The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007. Further information can be found on the Environment Agency website.
- Where any protected or restricted data has been held we get a certificate of secure deletion for any server that once contained personal data.

6. Equipment and Digital Content

Mobile Devices (Mobile phones, tablets and other mobile devices):

- Mobile devices brought into school are entirely at the staff member, students & parents or visitors own risk. The School accepts no responsibility for the loss, theft or damage of any phone or hand held device brought into school.
- All visitors are requested to keep their phones on silent.
- The recording, taking and sharing of images, video and audio on any personal mobile device is to be avoided, except where it has been explicitly agreed by the Headteacher. Such authorised use is to be recorded. All mobile device use is to be open to monitoring scrutiny and the Headteacher is able to withdraw or restrict authorisation for use at any time, if it is deemed necessary.
- The School reserves the right to search the content of any mobile devices on the school premises where there is a reasonable suspicion that it may contain illegal or undesirable material, including pornography, violence or bullying.

Storage, Synching and Access

The device is accessed with a school owned account

- The device has a school created account and all apps and file use is in line with this policy. No personal elements may be added to this device.
- PIN access to the device must always be known by the Head Teacher.

The device is accessed with a personal account

- If personal accounts are used for access to a school owned mobile device, staff must be aware that school use will be synched to their personal cloud, and personal use may become visible in school and in the classroom.
- PIN access to the device must always be known by the network manager.
- Exit process – when the device is returned the staff member must log in with personal ID so that the device can be Factory Reset and cleared for reuse.

Students' use of personal devices

- No students should bring his or her mobile phone or personally-owned device into school. Devices which are bought in must be handed in to SLT at the start of the day. Any device brought into school and not handed in will be confiscated.
- If a student breaches the school policy, then the device will be confiscated and will be held in a secure place in the school office. Mobile devices will be released to parents or carers in accordance with the school policy.
- Students should protect their phone numbers by only giving them to trusted friends and family members. Students will be instructed in safe and appropriate use of mobile phones and personally-owned devices and will be made aware of boundaries and consequences.
- If a student needs to contact his or her parents or carers, they will be allowed to use a school phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office.

Staff use of personal devices

- Staff are not permitted to use their own mobile phones or devices in a professional capacity, such as for contacting children, young people or their families within or outside of the setting.
- Staff will be issued with a school phone where contact with students, parents or carers is required, for instance for off-site activities.
- Personal mobile devices will not be used during lessons or formal school time unless as part of an approved and directed curriculum-based activity with consent from Headteacher / SLT. See Staff Handbook.
- Staff may use their phones during break times. If a staff member is expecting a personal call they may leave their phone with the school office to answer on their behalf, or seek specific permissions to use their phone at other than their break times.
- Staff should not use personally-owned devices, such as mobile phones or cameras, to take photos or videos of students and will only use work-provided equipment for this purpose.
- In an emergency where a staff member doesn't have access to a school-owned device, they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes and then report the incident with the Headteacher / Designated Officer.
- If a member of staff breaches the school policy then disciplinary action may be taken.

Digital images and video

In this school:

- We gain parental/carers permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter/son joins the school (or annually).
- We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials/DVDs.
- Staff sign the school's Acceptable Use Policy and this includes a clause on the use of mobile phones/personal equipment for taking pictures of pupils.
- If specific pupil photos (not group photos) are used on the school web site, in the prospectus or in other high profile publications the school will obtain individual parental or pupil permission for its long term.
- The school blocks/filter access to social networking sites unless there is a specific approved educational purpose.
- Pupils are taught about 'sexting' and the implications such images may have on their digital footprint and personal reputation.
- Pupils are taught about how images can be manipulated in their online safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children as part of their computing scheme of work.

- Pupils are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.
- Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.



Acceptable Use Agreement: All Staff, Volunteers and Governors

Covers use of all digital technologies in school: i.e. email, Internet, intranet, network resources, learning platform, software, communication tools, equipment and systems.

- I will only use the school's digital technology resources and systems for Professional purposes or for uses deemed 'reasonable' by the Head and Governing Body.
- I will not reveal my password(s) to anyone.
- I will follow 'good practice' advice in the creation and use of my password. If my password is compromised, I will ensure I change it. I will not use anyone else's password if they reveal it to me and will advise them to change it.
- I will not allow unauthorised individuals to access email / Internet / network, or other school systems, or any Local Authority (LA) system I have access to.
- I will ensure all documents, data etc., are printed, saved, accessed and deleted / shredded in accordance with the school's network and data security protocols.
- I will not engage in any online activity that may compromise my professional responsibilities.
- I will only use the approved email system(s) for any school business.
This is currently: LGFL Mail system
- I will only use the approved email system, Learning Platform (MLE) and school approved communication systems with pupils or parents/carers, and only communicate with them on appropriate school business.
- I will not browse, download or send material that is considered offensive or of an extremist nature by the school.
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach or equipment failure to the Child Protection Officer / NPW.
- I will not download any software or resources from the Internet that can compromise the network or might allow me to bypass the filtering and security system or are not adequately licensed.
- I will check copyright and not publish or distribute any work including images, music and videos, that is protected by copyright without seeking the author's permission.
- I will not connect any device (including USB flash drive), to the network that does not have up-to-date anti-virus software, and I will keep any 'loaned' equipment up-to-date, using the school's recommended anti-virus and other IT 'defence' systems.
- I will not use personal digital cameras or camera phones or digital devices for taking, editing and transferring images or videos of pupils or staff and will not store any such images or videos at home.
- I will follow the school's policy (Staff Handbook p24) on use of mobile phones / devices at school.



- I will only use school approved equipment for any storage, editing or transfer of digital images / videos and ensure I only save photographs and videos of children and staff on the appropriate system or staff-only drive within school.
- I will use the school's Learning Platform (MLE) in accordance with school protocols.
- I will ensure that any private social networking sites / blogs etc that I create or actively contribute to are not confused with my professional role.
- I will ensure, where used, I know how to use any social networking sites / tools securely, so as not to compromise my professional role.
- I agree and accept that any computer or laptop loaned to me by the school, is provided solely to support my professional responsibilities.
- I will only access school resources remotely (such as from home) using the LGfL / school approved system and follow e-security protocols to interact with them.
- I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow school data security protocols when using any such data at any location.
- I understand that data protection policy requires that any information seen by me with regard to staff or pupil information, held within the school's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.
- I will alert Essex Primary School child protection officer / appropriate senior member of staff if I feel the behaviour of any child may be a cause for concern.
- I understand it is my duty to support a whole-school safeguarding approach and will report any behaviour of other staff or pupils, which I believe may be inappropriate or concerning in any way, to senior member of staff / designated Child Protection lead.
- I understand that all Internet and network traffic / usage can be logged and this information can be made available to the Head / Safeguarding Lead on their request.
- I understand that Internet encrypted content (via the https protocol), may be scanned for security and/or safeguarding purposes.
- I will only use any LA system I have access to in accordance with their policies.
- Staff that have a teaching role only: I will embed the school's on-line safety / digital literacy / counter extremism curriculum into my teaching.



Acceptable Use Policy (AUP): Agreement Form

All Staff, Volunteers, Governors

User Signature

I agree to abide by all the points above.

I understand that I have a responsibility for my own and others online-safeguarding and I undertake to be a 'safe and responsible digital technologies user'.

I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school's most recent online-safety policies and appendices.

I understand that failure to comply with this agreement could lead to disciplinary action.

Signature Date

Full Name (printed)

Job title / Role

Authorised Signature (Head Teacher / Deputy)

I approve this user to be set-up on the school systems relevant to their role

Signature Date

Full Name (printed)

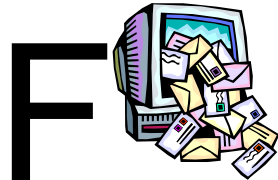
Think before you click



I will only use the Internet and email with an adult



I will only click on icons and links when I know they are safe



I will only send friendly and polite messages



If I see something I don't like on a screen, I will always tell an adult

My Name:

My Signature:



KS2 Pupil Acceptable Use Agreement

These rules will keep me safe and help me to be fair to others.

- I will only use the school's computers for schoolwork and homework.
- I will only edit or delete my own files and not look at, or change, other people's files without their permission.
- I will keep my logins and passwords secret.
- I will not bring files into school without permission or upload inappropriate material to my workspace.
- I am aware that some websites and social networks have age restrictions and I should respect this.
- I will not attempt to visit Internet sites that I know to be banned by the school.
- I will only e-mail people I know, or a responsible adult has approved.
- The messages I send, or information I upload, will always be polite and sensible.
- I will not open an attachment, or download a file, unless I know and trust the person who has sent it.
- I will not give my home address, phone number, send a photograph or video, or give any other personal information that could be used to identify me, my family or my friends, unless a trusted adult has given permission. I will never arrange to meet someone I have only ever previously met on the Internet, unless my parent/carer has given me permission and I take a responsible adult with me.
- If I see anything I am unhappy with or I receive a message I do not like, I will not respond to it but I will show a teacher / responsible adult.

I have read and understand these rules and agree to them.

Signed:

Date:



Appendix 3

Acceptable Use Agreement including photo/ video permission (parents)

Internet and IT: As the parent or legal guardian of the pupil(s) named below, I grant permission for the school to give my *daughter / son* access to:

- the Internet at school
- the school's chosen email system
- the school's online managed learning environment
- IT facilities and equipment at the school.



I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the Internet and mobile technologies, but I understand that the school takes every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials.



I understand that the school can, if necessary, check my child's computer files and the Internet sites they visit at school and if there are concerns about my child's online safety or online behaviour they will contact me.



Use of digital images, photography and video: I understand the school has a clear policy on "The use of digital images and video" and I support this.



I understand that the school will necessarily use photographs of my child or including them in video material to support learning activities.



I accept that the school may use photographs / video that includes my child in publicity that reasonably promotes the work of the school, and for no other purpose.



I will not take and then share online, photographs of other children (or staff) at school events without permission.



Social networking and media sites: I understand that the school has a clear policy on "The use of social networking and media sites" and I support this.



I understand that the school takes any inappropriate behaviour seriously and will respond to observed or reported inappropriate or unsafe behaviour.



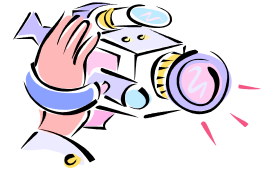
I will support the school by promoting safe use of the Internet and digital technology at home. I will inform the school if I have any concerns.



My daughter / son name(s): _____

Parent / guardian signature: _____

Date: ____/____/____



The use of digital images and video

To comply with the Data Protection Act 1998, we need your permission before we can photograph or make recordings of your daughter / son.

We follow the following rules for any external use of digital images:

If the pupil is named, we avoid using their photograph.

If their photograph is used, we avoid naming the pupil.

Where showcasing examples of pupils work we only use their first names, rather than their full names.

If showcasing digital video work to an external audience, we take care to ensure that pupils aren't referred to by name on the video, and that pupils' full names aren't given in credits at the end of the film.

Only images of pupils in suitable dress are used.

Staffs are not allowed to take photographs or videos on their personal equipment.

Examples of how digital photography and video may be used at school include:

- Your child being photographed (by the class teacher or teaching assistant) as part of a learning activity;
e.g. taking photos or a video of progress made by a nursery child, as part of the learning record, and then sharing with their parent / guardian.
- Your child's image being used for presentation purposes around the school;
e.g. in class or wider school wall displays or PowerPoint® presentations.
- Your child's image being used in a presentation about the school and its work in order to share its good practice and celebrate its achievements, which is shown to other parents, schools or educators;
e.g. within a CDROM / DVD or a document sharing good practice; in our school prospectus or on our school website.

In rare events, your child's picture could appear in the media if a newspaper photographer or television film crew attends an event.

Note: If we, or you, actually wanted your child's image linked to their name we would contact you separately for permission, e.g. if your child won a national competition and wanted to be named in local or government literature.



The use of social networking and on-line media

This school asks its whole community to promote the 3 commons approach to online behaviour:

- **Common courtesy**
- **Common decency**
- **Common sense**

How do we show common courtesy online?

- We ask someone's permission before uploading photographs, videos or any other information about them online.
- We do not write or upload 'off-hand', hurtful, rude or derogatory comments and materials. To do so is disrespectful and may upset, distress, bully or harass.

How do we show common decency online?

- We do not post comments that can be considered as being **intimidating, racist, sexist, homophobic or defamatory. This is cyber-bullying** and may be harassment or libel.
- When such comments exist online, we do not forward such emails, tweets, videos, etc. By creating or forwarding such materials we are all liable under the law.

How do we show common sense online?

- We think before we click.
- We think before we upload comments, photographs and videos.
- We think before we download or forward any materials.
- We think carefully about what information we share with others online, and we check where it is saved and check our privacy settings.
- We make sure we understand changes in use of any web sites we use.
- We block harassing communications and report any abuse.

Any actions online that impact on the school and can potentially lower the school's (or someone in the school) reputation in some way or are deemed as being inappropriate will be responded to.

In the event that any member of staff, student or parent/carer is found to be posting libellous or inflammatory comments on Facebook or other social network sites, they will be reported to the appropriate 'report abuse' section of the network site.

(All social network sites have clear rules about the content which can be posted on the site and they provide robust mechanisms to report contact or activity which breaches this.)

In serious cases we will also consider legal options to deal with any such misuse.

The whole school community is reminded of the CEOP report abuse process: <https://www.thinkuknow.co.uk/parents/browser-safety/>



DIGITALLY
CONFIDENT



**First Line Information
Support for Esafety
Incidents**



Esafety is a key element of safeguarding, subject to inspection by Ofsted and applies to adults and children of all ages.

The consequences of esafety incidents will cover a range of challenges, with consequences that range from those that may appear trivial to serious abuse and loss of life. This means First line colleagues must ensure that they treat all reports with appropriate professionalism and follow correct and agreed procedures.

This resource is intended to provide support for those who are new to esafety and first line support.

You are encouraged to regularly view digitallyconfident.org where we provide links to current news, opinion and resources in the areas of digital literacy and online safety.

We gratefully acknowledge the assistance of the following people in collating the following resources;

*Penny Patterson – London Grid for Learning
David Wright and Ken Corish – South West Grid for Learning
Alan Mackenzie – Independent esafety advisor*



Types of incidents



Predators

There will be cases where children will agree to meet face to face with abusers who they know or who have become 'friends' via online networks. Some children will be victims of emotional, sexual and physical abuse. There are cases where these relationships result in the death of a child.

Some children will be more vulnerable than others however it is important to recognise that all young people can seek comfort and friendship in online relationships. These relationships can appear more open, trusting and supportive than face to face interactions – and as such can pose new and different challenges and dangers.



Bullying & Cyberbullying

Cyberbullying typically takes two forms; by peers and strangers. Most common are the incidents where young people are bullied by other young people who are known to them in their school or wider community. There are incidents where individuals are victims of online bullying by strangers, members of the wider online communities and 'trolls'.

It is also important to note that adults who work with young people can be bullied and threatened by young people, parents and even colleagues.



Illegal or Inappropriate?

It is important to recognise the difference between illegal and inappropriate content and activity. For example; most pornography, whilst inappropriate within a school or work environment, is not illegal. Images of child exploitation (we do not use labels such as 'child pornography' – these images are child abuse and exploitation) are illegal. This can be complicated and sensitive where, for example, children under the age of eighteen are sharing sexual images of themselves. A young person is, in the UK, a child until the age of eighteen and it is understandable that there is ignorance around this when the age of consent is sixteen.

Young people need to be helped to understand that they are creating illegal content which will possibly lead to their friends and relatives becoming convicted and placed on the sex offenders register.

It is also worth noting that using the labels legal and illegal is not always helpful and it is more effective to ascertain; is the activity an offence?

This distinction is important and **if in doubt, err on the side of caution**. It is an offence to open, view, forward, copy and distribute images of child sex abuse. This means you must not forward or copy files and links to share with colleagues, authorities or the police.

Offence

- ⚠ Opening an attachment or URL that proves to hold illegal content is an illegal act and is classed as possession of illegal material.
- ⚠ Showing anyone else illegal material that you have received is an illegal act
- ⚠ Printing and sharing a copy of the material is an illegal act and is classed as distributing illegal material.

Not an Offence

- ⚠ Receiving unsolicited emails that may contain potentially illegal material (either as an attachment or in a URL) is not an illegal offence

Never open unsolicited URLs or attachments. If you are suspicious that the content could be illegal report it and log that you have received it.



Sexting and the law

1. You could end up with a police caution

Sending a naked image of yourself via text message, or social media, when you're below the age of 18 is technically illegal. It counts as an offence of distributing an indecent image of a child. You could even end up on the sex offenders register.

"The law doesn't distinguish between an indecent image of you and an indecent image of someone else."

2. It's worse to send a photo of a sexual act

Even though the age of sexual consent is 16, the age for distributing indecent images is 18. That means that a 17-year-old who can legally have sex cannot legally send a naked image. It's just as bad for a 15-year-old as a 17-year-old to sext.

But, what's worse for a 15-year-old is to send a photo showing them having sex. It's illegal for anyone below the age of 16 to have sex, so if the photo shows this, it could lead to them having doubly bad consequences.

If a 17-year-old sent a sext showing them having sex, they'd still be committing an offence by sending a naked image - but it wouldn't break the law around consent. A 15-year-old doing the same would be committing two offences.

3. An unwanted sext could be seen as a crime

But if you do send a naked selfie to someone who is likely to be upset by it, that could be a crime under the Malicious Communications Act.



Sexting and the law

4. Forwarding them on breaches civil law

“When you create a photo, as the creator you automatically become the owner of the copyright. Anyone who’s taking a risqué picture and sending it to their partner, they’ll own the copyright.”

If the receiver of the image then circulates it, or posts it on a website, they’re then infringing that copyright.

5. You could become a victim of revenge porn

One serious risk of sending explicit pictures is that someone could pass them on – either by circulating them or posting them onto a website. Once the pictures are there, it’s hard to get them taken down.

You could approach websites with claims of breaching harassment laws and copyright laws, but it’s often too late.

However someone who posts photos of an ex, perhaps, in a moment of anger, could be prosecuted for this.

6. You could break privacy law

Another issue with forwarding on images –

“We’d argue that communication was being made in the private constraints and any wider dissemination of that content would be breach of privacy.”

So...can you sext safely?

If you’re under 18, it is an offence to take and/or send a naked picture of yourself. It’s not illegal to be naked with someone, even if you’re 15, but you can’t send that picture.

As strange as it seems, it’s the law and it’s best to know the risks now.

Source:

www.telegraph.co.uk/women/womens-health/10985660/Sexting-scare-6-sexting-myths-busted.html


Responding to Sexting

In light of comments in September 2015 from the National Police Chief Council's lead on children and young people who said, "if a school chose to take an incident to the police, then officers must record the crime", we have updated our advice on how schools should manage incidents of sexting.

For Staff

If you have a report of (or you suspect) a sexting incident

Remember: intimate sexting images are typically considered to be illegal images which is why incidents need very careful management for all those involved.



If a device is involved – secure the device and switch it off

Seek advice - report to your designated child protection officer via your normal child protection procedures

“ Sexting doesn't just occur within, but also now happens prior to, a relationship
Prof A Phippen (2012) ”

“ 16% of teenagers don't think naked images are inappropriate
SWGfL (2009) ”

“ Teenagers typically consider sexting to be 'mundane' and widely known about ”

“ Celebrity, media representations of body image and pornography all play a role in sexting ”



¹Phippen, A. (2012) Sexting: An Exploration of Practices, Attitudes and Influences. (<https://www.nspcc.org.uk/globalassets/documents/research-reports/sexting-exploration-practices-attitudes-influences-report-2012.pdf>)

²http://ceop.police.uk/Documents/ceopdocs/externaldocs/ACPO_Lead_position_on_Self_Take_n_Images.pdf



UK Safer
Internet
Centre



SWGfL

Managing Sexting Incidents

In light of comments in September 2015 from the National Police Chief Council's lead on children and young people who said, "if a school chose to take an incident to the police, then officers must record the crime", we have updated our advice on how schools should manage incidents of sexting.



Designated child protection Officer

Sexting among children and young people can be a common occurrence; where they often describe these incidents as 'mundane'. Children, involved in sexting incidents, will be dealt with (by the police) as victims as opposed to perpetrators (unless there are mitigating circumstances).

Record all incidents of sexting. This includes both the actions you did take together with the actions that you didn't take, together with justifications.

In applying judgement to each sexting incident consider the following:

- ✓ Significant age difference between the sender/receiver involved.
- ✓ If there is any external coercion involved or encouragement beyond the sender/receiver.
- ✓ If you recognise the child as more vulnerable than is usual (ie at risk).
- ✓ If the image is of a severe or extreme nature.
- ✓ If the situation is not isolated and the image has been more widely distributed.
- ✓ If other knowledge of either the sender/recipient may add cause for concern (ie difficult home circumstances).

If you have a report of (or you suspect) a sexting incident



If these characteristics present cause for concern, then escalate or refer the incident using your normal child protection procedures.

If these characteristics do not present cause for concern, then manage the situation accordingly, recording details of the incident, action and resolution.

¹Phippen, A. (2012) Sexting: An Exploration of Practices, Attitudes and Influences. (<https://www.nspcc.org.uk/globalassets/documents/research-reports/sexting-exploration-practices-attitudes-influences-report-2012.pdf>)

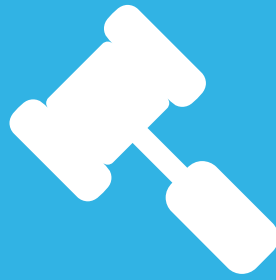
²http://ceop.police.uk/Documents/ceopdocs/externaldocs/ACPO_Lead_position_on_Self_Take_n_Images.pdf



UK Safer
Internet
Centre



SWGfL



The law with regard to illegal activity

Computer Misuse Act 1990

This Act makes it an offence to:

- Erase or amend data or programs without authority.
- Obtain unauthorised access to a computer.
- “Eavesdrop” on a computer.
- Make unauthorised use of computer time or facilities.
- Maliciously corrupt or erase data or programs.
- Deny access to authorised users.

Data Protection Act 1998

This protects the rights and privacy of individual’s data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully.

The Act states that personal data must be:

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant and not excessive.
- Accurate.
- Not kept longer than necessary.
- Processed in accordance with the data subject’s rights.
- Secure.
- Not transferred to other countries without adequate protection.

Freedom of Information Act 2000

The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.



The law with regard to illegal activity

Communications Act 2003

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Malicious Communications Act 1988

It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

Regulation of Investigatory Powers Act 2000

It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:

- Establish the facts;
- Ascertain compliance with regulatory or self-regulatory practices or procedures;
- Demonstrate standards, which are or ought to be achieved by persons using the system;
- Investigate or detect unauthorised use of the communications system;
- Prevent or detect crime or in the interests of national security;
- Ensure the effective operation of the system.
- Monitoring but not recording is also permissible in order to:
- Ascertain whether the communication is business or personal;
- Protect or support help line staff.
- The school reserves the right to monitor its systems and communications in line with its rights under this act.

Trade Marks Act 1994

This provides protection for Registered Trade Marks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trade Marks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.



The law with regard to illegal activity

Copyright, Designs and Patents Act 1988

It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. youtube).

Telecommunications Act 1984

It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

Criminal Justice & Public Order Act 1994

This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they:

- Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or
- Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

Racial and Religious Hatred Act 2006

This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.



The law with regard to illegal activity

Protection from Harrassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Protection of Children Act 1978

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison

Sexual Offences Act 2003

The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

Public Order Act 1986

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence. Children, Families and Education Directorate page 38 April 2007.



The law with regard to illegal activity

Obscene Publications Act 1959 and 1964

Publishing an “obscene” article is a criminal offence. Publishing includes electronic transmission.

Human Rights Act 1998

This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of “higher law”, affecting all other laws. In the school context, human rights to be aware of include:

- The right to a fair trial
- The right to respect for private and family life, home and correspondence
- Freedom of thought, conscience and religion
- Freedom of expression
- Freedom of assembly
- Prohibition of discrimination
- The right to education

These rights are not absolute. The school is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

The Education and Inspections Act 2006

Empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

The Education and Inspections Act 2011

Extended the powers included in the 2006 Act and gave permission for Headteachers (and nominated staff) to search for electronic devices. It also provides powers to search for data on those devices and to delete data.

(see template policy in these appendices and for DfE guidance -

www.education.gov.uk/schools/pupilsupport/behaviour/behaviourpolicies/f0076897/screening-searching-and-confiscation)



The law with regard to illegal activity

The Protection of Freedoms Act 2012

Requires schools to seek permission from a parent / carer to use Biometric systems.

The School Information Regulations 2012

Requires schools to publish certain information on its website:

www.education.gov.uk/schools/toolsandinitiatives/cuttingburdens/b0075738/reducing-bureaucracy/requirements/changestoschoolinformationregulations



Dealing with a device where there is suspicion of illegal content

It is advised that if there is suspicion of something illegal on a school device (and this would now also relate to a device brought in by a student), then the device is to be powered off at the plug (not Shut Down), locked away in a secure cabinet and nobody allowed to access that cabinet until the police have arrived and determined, upon investigation, whether the device warrants seizure or not.

As many devices such as phones, tablets and laptops have their own power supply via a battery, the advice to power off via the mains supply is not relevant. In such cases the device can be turned off and secured immediately in a safe location to ensure no one has further access to it prior to investigation.

It is also good practice that when the member of staff seizes the device they record the date and time.

We can see in the following materials by SWGFL that the decision to search a student or adult's device must be made with care. There is a balance between infringing people's rights and protecting the individual. With this in mind it would be prudent to ensure that responsible individuals (Senior leaders and those with responsibility for safeguarding and safety) follow an agreed and documented procedure to search a device. The act of searching a personal device may be seen as sensitive as a physical search of the child or adult involved.



Dealing with a device where there is suspicion of illegal content

Extract from SWGfL School E-Safety Policy Template Document

The Education Act 2012, the basis of this template, sets out what the law is presumed to be, based on prior legal and educational knowledge, and common sense. Rights and responsibilities regarding physical contact and personal data are still evolving rapidly. So too are social, entertainment and educational technologies and the skills necessary to use them safely and prudently. This is particularly so where those who are under 18 are involved.

No existing law or policy can fully insulate anyone from the risk involved in searching for, access to or deletion of the personal data of others. Anyone refraining from any such search, access or deletion when hindsight shows circumstances merit such actions may however be at significant risk and may put seriously at risk the wellbeing of children entrusted to their care. This template cannot therefore be relied on as justification for any act or lack of action by anyone – there is no substitute for the proper and well documented exercise of adequately informed professional judgement. .

It is for each school's / academy's Headteacher / Principal and Governors / Directors to set, apply and monitor application of their own policies as guided by their head teacher, local authority and official guidance, especially if the school is local authority maintained. This template is intended as an aide to this. South West Grid for Learning Trust does not and cannot accept and does not have responsibility for any school's policy on this or any other matter.

Where sections in the template are written in ITALICS it is anticipated that schools would wish to consider whether or not to include that section or statement in their completed policy.

Where sections are highlighted in BOLD text, it is the view of the SWGfL E-Safety Group that these ought to be an essential part of a school e-safety policy.

The template uses the term students / pupils to refer to the children / young people attending the learning institution and the term Headteacher / Principal. Schools will need to choose which terms to use and delete the others accordingly.



Dealing with a device where there is suspicion of illegal content

Extract from SWGfL School E-Safety Policy Template Document

Introduction

The changing face of information technologies and ever increasing pupil / student use of these technologies has meant that the Education Acts have had to change in an attempt to keep pace. Within Part 2 of the Education Act 2011 (Discipline) there have been changes to the powers afforded to schools by statute to search pupils in order to maintain discipline and ensure safety. Schools are required to ensure they have updated policies which take these changes into account. No such policy can on its own guarantee that the school will not face legal challenge, but having a robust policy which takes account of the Act and applying it in practice will however help to provide the school with justification for what it does.

The particular changes we deal with here are the added power to search for items 'banned under the school rules' and the power to 'delete data' stored on seized electronic devices.

Items banned under the school rules are determined and publicised by the Headteacher (section 89 Education and Inspections Act 1996).

An item banned by the school rules may only be searched for under these new powers if it has been identified in the school rules as an item that can be searched for. It is therefore important that there is a school policy which sets out clearly and unambiguously the items which:

- are banned under the school rules; and
- are banned AND can be searched for by authorised school staff

The act allows authorised persons to examine data on electronic devices if they think there is a good reason to do so. In determining a 'good reason' to examine or erase the data or files the authorised staff member must reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or could break the school rules.

Following an examination, if the person has decided to return the device to the owner, or to retain or dispose of it, they may erase any data or files, if they think there is a good reason to do so.

The Head Teacher / Principal must publicise the school

behaviour policy, in writing, to staff, parents / carers and students / pupils at least once a year. (There should therefore be clear links between the search etc. policy and the behaviour policy).

DfE advice on these sections of the Education Act 2011 can be found in the document: "Screening, searching and confiscation – Advice for head teachers, staff and governing bodies"

www.education.gov.uk/schools/pupilsupport/behaviour/behaviourpolicies/f0076897/screening-searching-and-confiscation

It is recommended that Headteachers / Principals (and, at the least, other senior leaders) should be familiar with this guidance.

Relevant legislation:

- Education Act 1996
- Education and Inspections Act 2006
- Education Act 2011 Part 2 (Discipline)
- The School Behaviour (Determination and Publicising of Measures in Academies) Regulations 2012
- Health and Safety at Work etc. Act 1974
- Obscene Publications Act 1959
- Children Act 1989
- Human Rights Act 1998
- Computer Misuse Act 1990

This is not a full list of Acts involved in the formation of this advice. Further information about relevant legislation can be found via the above link to the DfE advice document.



Dealing with a device where there is suspicion of illegal content

Extract from SWGfL School E-Safety Policy Template Document

Responsibilities

The Headteacher / Principal is responsible for ensuring that the school policies reflect the requirements contained within the relevant legislation. The formulation of these policies may be delegated to other individuals or groups. The policies will normally be taken to Governors for approval. The Headteacher/ Principal will need to authorise those staff who are allowed to carry out searches.

This policy has been written by and will be reviewed by: [insert relevant names / roles / group]

The Headteacher / Principal has authorised the following members of staff to carry out searches for and of electronic devices and the deletion of data / files on those devices: (the policy should here list those staff / roles given such authority. A Headteacher / Principal may choose to authorise all staff willing to be authorised, but should consider training needs in making this decision).

The Headteacher / Principal may authorise other staff members in writing in advance of any search they may undertake, subject to appropriate training.

Members of staff (other than Security Staff) cannot be required to carry out such searches. They can each choose whether or not they wish to be an authorised member of staff.

Members of staff authorised by the Headteacher / Principal to carry out searches for and of electronic devices and to access and delete data / files from those devices should receive training that is specific and relevant to this role.

Specific training is required for those staff who may need to judge whether material that is accessed is inappropriate or illegal.

Training / Awareness

It is essential that all staff should be made aware of and should implement the school's policy.

Members of staff should be made aware of the school's policy on "Electronic devices – searching and deletion":

- at induction
- at regular updating sessions on the school's e-safety policy



Dealing with a device where there is suspicion of illegal content

Extract from SWGfL School E-Safety Policy Template Document

Policy Statements relating to searching devices

The school Behaviour Policy refers to the policy regarding searches with and without consent for the wide range of items covered within the Education Act 2011 and lists those items. This policy refers only to the searching for and of electronic devices and the deletion of data / files on those devices.

The school will already have a policy relating to whether or not mobile phones and other electronic devices are banned, or are allowed only within certain conditions. The school should therefore consider including one of the following statements in the policy:

EITHER

Pupils/students are not allowed to bring mobile phones or other personal electronic devices to school or use them in the school.

OR

Pupils / students are allowed to bring mobile phones or other personal electronic devices to school and use them only within the rules laid down by the school. (you should refer to the relevant policy or to list here the conditions under which they are allowed)

IF PUPILS/STUDENTS BREACH THESE RULES:

EITHER

The sanctions for breaking these rules will be: [list here]

OR

The sanctions for breaking these rules can be found in the [name the policy - for many schools this will be the Behaviour Policy]

Authorised staff (defined in the responsibilities section above) have the right to search for such electronic devices where they reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or break the school rules.

- Searching with consent - Authorised staff may search with the pupil's consent for any item.
- Searching without consent - Authorised staff may only search without the pupil's consent for anything which is either 'prohibited' (as defined in Section 550AA of the Education Act 1996) or appears in the school rules as an item which is banned and may be searched for.

IN CARRYING OUT THE SEARCH

The authorised member of staff must have reasonable grounds for suspecting that a student / pupil is in possession of a prohibited item i.e. an item banned by the school rules and which can be searched for. (Whether there are 'reasonable grounds' is a matter decided on by reference to the circumstances witnessed by, or reported to, someone who is authorised and who exercises properly informed professional judgment and has received appropriate training).

The authorised member of staff should take reasonable steps to check the ownership of the mobile phone / personal electronic device before carrying out a search. (The powers included in the Education Act do not extend to devices owned (or mislaid) by other parties eg



Dealing with a device where there is suspicion of illegal content

Extract from SWGfL School E-Safety Policy Template Document

a visiting parent or contractor, only to devices in the possession of pupils / students.)

The authorised member of staff should take care that, where possible, searches should not take place in public places e.g. an occupied classroom, which might be considered as exploiting the student / pupil being searched.

The authorised member of staff carrying out the search must be the same gender as the student / pupil being searched; and there must be a witness (also a staff member) and, if at all possible, they too should be the same gender as the student / pupil being searched.

There is a limited exception to this rule: Authorised staff can carry out a search of a student / pupil of the opposite gender including without a witness present, **but only where you reasonably believe that there is a risk that serious harm will be caused to a person if you do not conduct the search immediately and where it is not reasonably practicable to summon another member of staff.**

EXTENT OF THE SEARCH

The person conducting the search may not require the student/ pupil to remove any clothing other than outer clothing.

Outer clothing means clothing that is not worn next to the skin or immediately over a garment that is being worn as underwear (outer clothing includes hats; shoes; boots; coat; blazer; jacket; gloves and scarves).

‘Possessions’ means any goods over which the student / pupil has or appears to have control – this includes desks, lockers and bags. (schools will need to take account of their normal policies regarding religious garments / headwear and may wish to refer to it in this policy)

A student’s / pupil’s possessions can only be searched in the presence of the student / pupil and another member of staff, except where there is a risk that serious harm will be caused

to a person if the search is not conducted immediately and where it is not reasonably practicable to summon another member of staff.

The power to search without consent enables a personal search, involving removal of outer clothing and searching of pockets; but not an intimate search going further than that, which only a person with more extensive powers (e.g. a police officer) can do.

Use of Force – force cannot be used to search without consent for items banned under the school rules regardless of whether the rules say an item can be searched for.

Further information relating to searching students can be found in this Department of Education document (published Feb 14)
www.gov.uk/government/publications/searching-screening-and-confiscation

ELECTRONIC DEVICES

An authorised member of staff finding an electronic device may access and examine any data or files on the device if they think there is a good reason to do so (i.e. the staff member must reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or break the school rules).

The examination of the data / files on the device should go only as far as is reasonably necessary to establish the facts of the incident. Any further intrusive examination of personal data may leave the school open to legal challenge. It is important that authorised staff should have training and sufficient knowledge of electronic devices and data storage.



Dealing with a device where there is suspicion of illegal content

Extract from SWGfL School E-Safety Policy Template Document

If inappropriate material is found on the device it is up to the authorised member of staff to decide whether they should delete that material, retain it as evidence (of a criminal offence or a breach of school discipline) or whether the material is of such seriousness that it requires the involvement of the police.

Examples of illegal activity would include:

- child sexual abuse images (including images of one child held by another child)
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials

Members of staff may require support in judging whether the material is inappropriate or illegal. One or more Senior Leaders should receive additional training to assist with these decisions. Care should be taken not to delete material that might be required in a potential criminal investigation.

The school should also consider their duty of care responsibility in relation to those staff who may access disturbing images or other inappropriate material whilst undertaking a search. Seeing such material can be most upsetting. There should be arrangements in place to support such staff. The school may wish to add further detail about these arrangements.

Further guidance on reporting the incident to the police and the preservation of evidence can be found in the SWGfL flow chart in the main School Template Policies document. Local authorities / LSCBs may also have further guidance, specific to their area.

DELETION OF DATA

Following an examination of an electronic device, if the authorised member of staff has decided to return the device to the owner, or to retain or dispose of it, they may erase any data

or files, if they think there is a good reason to do so. (i.e. the staff member must reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or break the school rules).

A record should be kept of the reasons for the deletion of data / files. (DfE guidance states and other legal advice recommends that there is no legal reason to do this, best practice suggests that the school can refer to relevant documentation created at the time of any search or data deletion in the event of a pupil /student, parental or other interested party complaint or legal challenge. Records will also help the school to review e-safety incidents, learn from what has happened and adapt and report on application of policies as necessary).

CARE OF CONFISCATED DEVICES

School staff are reminded of the need to ensure the safe keeping of confiscated devices, to avoid the risk of compensation claims for damage / loss of such devices (particularly given the possible high value of some of these devices).

The school may wish to add a disclaimer to the relevant section of the Behaviour Policy which may assist in covering the school against damage / loss claims.

AUDIT / MONITORING / REPORTING / REVIEW

The responsible person [insert title] will ensure that full records are kept of incidents involving the searching for and of mobile phones and electronic devices and the deletion of data / files. (a template log sheet can be found in the



Dealing with a device where there is suspicion of illegal content

Extract from SWGfL School E-Safety Policy Template Document

appendices to the School E-Safety Template Policies)

These records will be reviewed by ... [E-Safety Officer / E-Safety Committee / E-Safety Governor] at regular intervals [state the frequency].

This policy will be reviewed by the head teacher and governors annually and in response to changes in guidance (DfE guidance will be reviewed in 2013) and evidence gained from the records.

The school is required to publish its Behaviour Policy to parents annually (including on its website) – the Behaviour Policy should be cross referenced with this policy on search and deletion.



E safety Log

Schools must have rigorous and meaningful reporting procedures in place and this includes an esafety log. The purpose of the log is to record all illegal/inappropriate/accidental/deliberate incidents. The log ensures that appropriate action is taken and child safeguarding is the priority. Over time the log will also act to inform policy and practice reviews by highlighting the types and frequency of incidents. Training and teaching can then be set in place to help minimise the likelihood of similar incidents in future.

Further to completing the incident log, all adults involved in the reporting process should email a brief summary of the incident to the headteacher. This means that they have a time/date stamped record of when they notified their headteacher, and leaves a clear audit trail for future reference if required.



E safety Log

Example esafety incident log

[school name] - Esafety Incident Log

Details of ALL esafety incidents to be recorded by the esafety Coordinator. This incident log will be monitored termly by the Headteacher, Member of SLT or Chair of Governors.

Date & Time	Name of pupil or staff member	Room and computer / device number	Details of incident (including evidence)	Actions	Name and role of person completing this entry

Record of reviewing devices / internet sites (responding to incidents of misuse)

Group	
Date	
Reason for investigation	

Details of first reviewing person

Name	
Position	
Signature	

Details of second reviewing person

Name	
Position	
Signature	

Name and location of computer used for review (for web sites)

--

Web site(s) address / device Reason for concern

Conclusion Action proposed or taken



Managing incidents

Thanks to Hertfordshire County Council and Southwest Grid
For Learning for their assistance and resources

For Headteachers, Senior Leaders and Governors

Involving staff as victims

All incidents should be reported to the Headteacher and/or Governors who will:

- ⚠ Record in the school esafety Incident Log
- ⚠ Keep any evidence – printouts and/ screen shots
- ⚠ Use the 'Report Abuse' button, if appropriate
- ⚠ Consider involving the Chair of Governors and /or reporting the incident to the Governing Body

Parents/carers as instigators

Contact the person and invite into school and discuss using some of the examples below:

- ⚠ You have become aware of discussions taking place online ...
- ⚠ You want to discuss this..
- ⚠ You have an open door policy so disappointed they did not approach you first



Managing incidents

- ⚠ They have signed the Home School Agreement which clearly states ...
- ⚠ Request the offending material be removed

If this does not solve the problem:

- ⚠ Consider involving the Chair of Governors
- ⚠ Consider involving the police (Communications Act 2003 & Malicious Communications Act 1988)

Staff/colleagues as instigators

Contact Schools HR for initial Advice and/ or contact Schools esafety Adviser In all serious cases this is the first step.

- ⚠ Contact the member of staff and request the offending material be removed immediately, (in serious cases you may be advised not to discuss the incident with the staff member)
- ⚠ Refer to the signed ICT Acceptable Use Agreement, Professional Code of Conduct and consider if this incident has an impact on the Contract of Employment of the member of staff.
- ⚠ Provide additional training
- ⚠ Invoke disciplinary procedures

Pupils as instigators

Follow some of the steps below:

- ⚠ Identify the pupils involved
- ⚠ Ask pupil to remove offensive material. Refer to the signed Acceptable Use Agreement.
- ⚠ If the perpetrator refuses to remove the material and is under 13 contact the Social Network who will close the account



Managing incidents

- ⚠ Take appropriate actions inline with school policies/ rules
- ⚠ Inform parents/ carers if serious or persistent incident
- ⚠ For serious incidents or further advice:
- ⚠ Inform your Local Police Safer Neighbourhood team
- ⚠ Local authority support services re bullying
- ⚠ If the child is at risk inform your school Child Protection Officer

Further Support

- ⚠ School HR contact [insert details]
- ⚠ Governor Services [insert details]
- ⚠ Teachers' union [insert details]
- ⚠ Police [insert details]
- ⚠ Local Authority HR, Legal, School Improvement Service [insert details]
- ⚠ **Where a child is believed to be at risk, contact Child Protection officer/ team. [insert details]**



Illegal Esafety Incident

For Headteachers, Senior Leaders and Governors

Examples of illegal activity/content

- ⚠ Downloading child abuse images/files
- ⚠ Sharing images or video containing child abuse
- ⚠ Inciting racial or religious hatred
- ⚠ Extreme cases of Cyberbullying
- ⚠ Promoting illegal acts

If illegal material or activity found or suspected:

- ⚠ Isolate device securely. (do not view or share content)
- ⚠ Inform esafety officer, SLT, Police, Chair of governors, LA School Improvement Leader (insert contact details)
- ⚠ If a student is involved notify Child Protection Officer
- ⚠ If a member of staff is involved contact LA Designated Officer for allegations against staff.



Non illegal Esafety Incident

For Headteachers, Senior Leaders and Governors

Involving staff as victims

Incident could be:

- ⚠ Using another person's password, online identity or log on details.
- ⚠ Accessing websites which are against school policy e.g. games, social networks.
- ⚠ Using a mobile phone to take video during a lesson.
- ⚠ Using the technology or social media to upset or bully or bring the individual, profession or organisation into disrepute.

If member of staff has:

- ⚠ Behaved in a way that has harmed a child, or may have harmed a child.
- ⚠ Possibly committed a criminal offence against or related to a child; or
- ⚠ Behaved towards a child or children in a way that indicates he or she would pose a risk of harm if they work regularly or closely with children.
- ⚠ Contact the LADO on: [insert number]
- ⚠ Review evidence and determine if the incident is accidental or deliberate
- ⚠ Decide upon the appropriate course of action
- ⚠ Follow school disciplinary procedures



Non illegal Esafety Incident

Pupils as instigators

- ⚠ Review incident and identify if other pupils were involved
- ⚠ Decide appropriate sanctions and/ or support based on school rules/ guidelines Inform parents/ carers if serious or persistent incident. In serious incidents consider informing the Child Protection Officer as the child instigator could be at risk
- ⚠ Review school procedures/policies to develop best practice

Pupils as victims

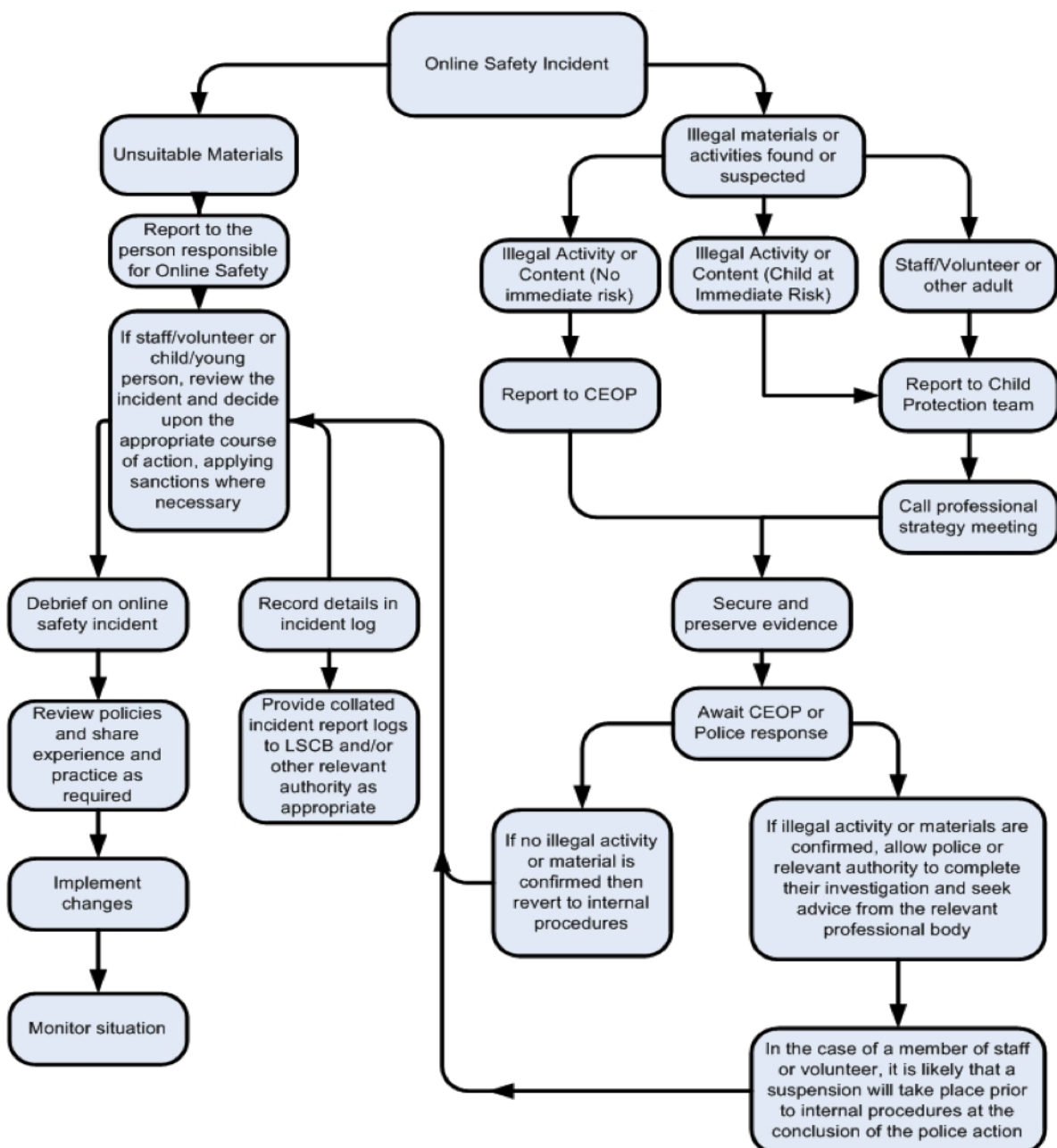
In –school action to support pupil by one or more of the following:

- ⚠ Class teacher
- ⚠ Esafety Coordinator
- ⚠ Senior Leader or Headteacher
- ⚠ Designated Senior Person for Child Protection (DSP)
- ⚠ School Police Community Support Officer

Then do the following:

- ⚠ Inform parents/ carer as appropriate.
- ⚠ If the child is at risk inform CSPLO immediately.
- ⚠ Confiscate the device, if appropriate.

SWFgL Esafety School Template Policies



Useful Links

Digitally Confident

www.digitallyconfident.org

South West Grid for Learning

www.swgfl.org.uk/Staying-safe

Childnet

www.childnet.com

Thinkyouknow

www.thinkyouknow.co.uk

Internet Watch Foundation

www.iwf.org.uk

CEOP

<http://ceop.police.uk>

Beat Bullying

www.beatbullying.org/gb/who-is-on-this-site

Reporting links for popular online services

<http://cyberbullying.us/report>

Guidelines on prosecuting cases involving communications sent via social media

www.cps.gov.uk/legal/a_to_c/communications_sent_via_social_media

Dealing with indecent images of children in the workplace: A Best Practice Guide

www.iwf.org.uk/resources/best-practice-guide



First Line Information Support for Esafety Incidents

MADE BY PHILIP & SIMON AT
www.digitallyconfident.org



Appendix 4: How will infringements be handled?

Whenever a student or staff member infringes the Online-Safety Policy, the final decision on the level of sanction will be at the discretion of the school management and will reflect the school's behaviour and disciplinary procedures.

The following are provided as **exemplification** only:

STUDENT	
Category A infringements	Possible Sanctions:
<ul style="list-style-type: none"> • Use of non-educational sites during lessons • Unauthorised use of email • Unauthorised use of mobile phone (or other new technologies) in lessons e.g. to send texts to friends • Use of unauthorised instant messaging / social networking sites 	<p>Refer to class teacher / tutor</p> <p>Escalate to: senior manager / Online-Safety Coordinator</p>
Category B infringements	Possible Sanctions:
<ul style="list-style-type: none"> • Continued use of non-educational sites during lessons after being warned • Continued unauthorised use of email after being warned • Continued unauthorised use of mobile phone (or other new technologies) after being warned • Continued use of unauthorised instant messaging / chatrooms, social networking sites, NewsGroups • Use of Filesharing software e.g. Napster, Vanbasco, BitTorrent, LiveWire, etc • Trying to buy items over online • Accidentally corrupting or destroying others' data without notifying a member of staff of it • Accidentally accessing offensive material and not logging off or notifying a member of staff of it 	<p>Refer to Class teacher/ Head of Department / Year tutor / Online-Safety Coordinator</p> <p>Escalate to:</p> <p>removal of Internet access rights for a period / removal of phone until end of day / contact with parent]</p>

STUDENT	
Category C infringements	Possible Sanctions:
<ul style="list-style-type: none"> Deliberately corrupting or destroying someone's data, violating privacy of others or posts inappropriate messages, videos or images on a social networking site. Sending an email or MSN message that is regarded as harassment or of a bullying nature (one-off) Trying to access offensive or pornographic material (one-off) Purchasing or ordering of items online Transmission of commercial or advertising material 	<p>Refer to Class teacher / Year Tutor / Online-Safety Coordinator / Head teacher / removal of Internet and/or Learning Platform access rights for a period</p> <p>Escalate to: contact with parents / removal of equipment</p> <p>Other safeguarding actions if inappropriate web material is accessed: Ensure appropriate technical support filters the site</p>
Category D infringements	Possible Sanctions:
<ul style="list-style-type: none"> Continued sending of emails or MSN messages regarded as harassment or of a bullying nature after being warned Deliberately creating accessing, downloading or disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988 Bringing the school name into disrepute 	<p>Refer to Head Teacher / Contact with parents</p> <p>Other possible safeguarding actions:</p> <ul style="list-style-type: none"> Secure and preserve any evidence Inform the sender's e-mail service provider. Liaise with relevant service providers/ instigators of the offending material to remove Report to Police / CEOP where child abuse or illegal activity is suspected

STAFF	
Category A infringements (Misconduct)	Possible Sanctions:
<ul style="list-style-type: none"> Excessive use of Internet for personal activities not related to professional development e.g. online shopping, personal email, instant messaging etc. Use of personal data storage media (e.g. USB memory sticks) without considering access and appropriateness of any files stored. Not implementing appropriate safeguarding procedures. Any behaviour on the World Wide Web that compromises the staff members professional standing in the school and community. Misuse of first level data security, e.g. wrongful use of passwords. Breaching copyright or license e.g. installing unlicensed software on network. 	<p>Referred to line manager / Head teacher</p> <p>Escalate to:</p> <p><i>Warning given</i></p>
Category B infringements (Gross Misconduct)	Possible Sanctions:
<ul style="list-style-type: none"> Serious misuse of, or deliberate damage to, any school / Council computer hardware or software; Any deliberate attempt to breach data protection or computer security rules; Deliberately creating ,accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent; Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988; Bringing the school name into disrepute 	<p>Referred to Head teacher / Governors;</p> <p>Other safeguarding actions:</p> <ul style="list-style-type: none"> Remove the PC to a secure place to ensure that there is no further access to the PC or laptop. Instigate an audit of all ICT equipment by an outside agency, such as the schools ICT managed service providers - to ensure there is no risk of pupils accessing inappropriate materials in the school. Identify the precise details of the material. <p><i>Escalate to:</i></p> <p><i>report to LA /LSCB, Personnel, Human resource.</i></p> <p>Report to Police / CEOP where child abuse or illegal activity is suspected. ,</p>

If a member of staff commits an exceptionally serious act of gross misconduct

The member of staff should be instantly suspended. Normally though, there will be an investigation before disciplinary action is taken for any alleged offence. As part of that the member of staff will be asked to explain their actions and these will be considered before any disciplinary action is taken.

Schools are likely to involve external support agencies as part of these investigations e.g. an ICT technical support service to investigate equipment and data evidence, the Local Authority Human Resources team.

Child abuse images found

In the case of Child abuse images being found, the member of staff should be **immediately suspended** and the Police should be called.

Anyone may report any inappropriate or potentially illegal activity or abuse with or towards a child online to the Child Exploitation and Online Protection (CEOP):

http://www.ceop.gov.uk/reporting_abuse.html

<http://www.iwf.org.uk>

How will staff and students be informed of these procedures?

- They will be fully explained and included within the school's Online-Safety / Acceptable Use Policy. All staff will be required to sign the school's online-safety acceptable use agreement form;
- Pupils will be taught about responsible and acceptable use and given strategies to deal with incidents so they can develop 'safe behaviours'. Pupils will sign an age appropriate online-safety / acceptable use agreement form;
- The school's online-safety policy will be made available and explained to parents, and parents will sign an acceptance form when their child starts at the school.
- Information on reporting abuse / bullying etc will be made available by the school for pupils, staff and parents.
- Staff are issued with the 'What to do if?' guide on online-safety issues, (see LGfL safety site).

Sample agreement forms can be downloaded from the LGfL online-safety site



HM Government

Prevent Duty Guidance: for England and Wales

Guidance for specified authorities in England and Wales on the duty in the Counter-Terrorism and Security Act 2015 to have due regard to the need to prevent people from being drawn into terrorism.

© Crown Copyright 2015

The text in this document (excluding the Royal Arms and other departmental or agency logos) may be reproduced free of charge in any format or medium providing it is reproduced accurately and not used in a misleading context. The material must be acknowledged as Crown copyright and the title of the document specified.

Where we have identified any third party copyright material you will need to obtain permission from the copyright holders concerned.

ISBN: 978-1-78246-7933-9

Contents

A. Status and Scope of the Duty.....	2
B. Introduction.....	2
C. A risk-based response to the <i>Prevent</i> duty.....	3
D. Monitoring and enforcement.....	5
E. Sector-specific guidance.....	6
Local authorities.....	6
Schools (excluding higher and further education).....	10
Further education.....	13
Higher education.....	16
The health sector.....	19
Prisons and probation.....	21
The police.....	25
F. Glossary of terms.....	27

A. Status and Scope of the Duty

Statutory guidance issued under section 29 of the Counter-Terrorism and Security Act 2015.

1. Section 26 of the Counter-Terrorism and Security Act 2015 (the Act) places a duty on certain bodies (“specified authorities” listed in Schedule 6 to the Act), in the exercise of their functions, to have “due regard to the need to prevent people from being drawn into terrorism”. This guidance is issued under section 29 of the Act. The Act states that the authorities subject to the provisions must have regard to this guidance when carrying out the duty.

2. The list of specified authorities subject to the provisions can be found in Schedule 6 to the Act. Further details can be found in the sector-specific sections of this guidance.

3. The duty applies to specified authorities in England and Wales, and Scotland. Counter terrorism is the responsibility of the UK Government. However, many of the local delivery mechanisms in Wales and Scotland, such as health, education and local government, are devolved. We will ensure close cooperation with the Scottish and Welsh Governments in implementing the Prevent duty where there are interdependencies between devolved and non-devolved elements. There is separate guidance for specified authorities in Scotland.

4. The duty does not confer new functions on any specified authority. The term “due regard” as used in the Act means that the authorities should place an appropriate amount of weight on the need to prevent people being drawn into terrorism when they consider all the other factors relevant to how they carry out their usual functions. This purpose of this guidance is to assist authorities to decide what this means in practice.

B. Introduction

5. The Prevent strategy, published by the Government in 2011, is part of our overall counter-terrorism strategy, CONTEST. The aim of the *Prevent* strategy is to reduce the threat to the UK from terrorism by stopping people becoming terrorists or supporting terrorism. In the Act this has simply been expressed as the need to “prevent people from being drawn into terrorism”.

6. The 2011 *Prevent* strategy has three specific strategic objectives:

- respond to the ideological challenge of terrorism and the threat we face from those who promote it;

- prevent people from being drawn into terrorism and ensure that they are given appropriate advice and support; and
- work with sectors and institutions where there are risks of radicalisation that we need to address.

7. Terrorist groups often draw on extremist ideology, developed by extremist organisations. Some people who join terrorist groups have previously been members of extremist organisations and have been radicalised by them. The Government has defined extremism in the *Prevent* strategy as: “vocal or active opposition to fundamental British values, including democracy, the rule of law, individual liberty and mutual respect and tolerance of different faiths and beliefs. We also include in our definition of extremism calls for the death of members of our armed forces”.

8. The *Prevent* strategy was explicitly changed in 2011 to deal with all forms of terrorism and with non-violent extremism, which can create an atmosphere conducive to terrorism and can popularise views which terrorists then exploit. It also made clear that preventing people becoming terrorists or supporting terrorism requires challenge to extremist ideas where they are used to legitimise terrorism and are shared by terrorist groups. And the strategy also means intervening to stop people moving from extremist (albeit legal) groups into terrorist-related activity.

9. Our *Prevent* work is intended to deal with all kinds of terrorist threats to the UK. The most significant of these threats is currently from terrorist organisations in Syria and Iraq, and Al Qa'ida associated groups. But terrorists associated with the extreme right also pose a continued threat to our safety and security.

10. Islamist extremists regard Western intervention in Muslim-majority countries as a 'war with Islam', creating a narrative of 'them' and 'us'. Their ideology includes the uncompromising belief that people cannot be both Muslim and British, and that Muslims living here should not participate in our democracy. Islamist extremists specifically attack the

principles of civic participation and social cohesion. These extremists purport to identify grievances to which terrorist organisations then claim to have a solution.

11. The white supremacist ideology of extreme right-wing groups has also provided both the inspiration and justification for people who have committed extreme right-wing terrorist acts.

12. In fulfilling the duty in section 26 of the Act, we expect all specified authorities to participate fully in work to prevent people from being drawn into terrorism. How they do this, and the extent to which they do this, will depend on many factors, for example, the age of the individual, how much interaction they have with them, etc. The specified authorities in Schedule 6 to the Act are those judged to have a role in protecting vulnerable people and/or our national security. The duty is likely to be relevant to fulfilling other responsibilities such as the duty arising from section 149 of the Equality Act 2010.

13. This guidance identifies best practice for each of the main sectors and describes ways in which they can comply with the duty. It includes sources of further advice and provides information on how compliance with the duty will be monitored.

C. A risk-based approach to the *Prevent* duty

14. In complying with the duty all specified authorities, as a starting point, should demonstrate an awareness and understanding of the risk of radicalisation in their area, institution or body. This risk will vary greatly and can change rapidly; but no area, institution or body is risk free. Whilst the type and scale of activity that will address the risk will vary, all specified authorities will need to give due consideration to it.

15. There are three themes throughout the sector-specific guidance, set out later in this document: effective leadership, working in partnership and appropriate capabilities.

Leadership

16. For all specified authorities, we expect that those in leadership positions:

- establish or use existing mechanisms for understanding the risk of radicalisation;
- ensure staff understand the risk and build the capabilities to deal with it;
- communicate and promote the importance of the duty; and
- ensure staff implement the duty effectively.

Working in partnership

17. Prevent work depends on effective partnership. To demonstrate effective compliance with the duty, specified authorities must demonstrate evidence of productive co-operation, in particular with local Prevent co-ordinators, the police and local authorities, and co-ordination through existing multi-agency forums, for example Community Safety Partnerships.

Capabilities

18. Frontline staff who engage with the public should understand what radicalisation means and why people may be vulnerable to being drawn into terrorism as a consequence of it. They need to be aware of what we mean by the term “extremism” and the relationship between extremism and terrorism (see section B, above).

19. Staff need to know what measures are available to prevent people from becoming drawn into terrorism and how to challenge the extremist ideology that can be associated with it. They need to understand how to obtain support for people who may be being exploited by radicalising influences.

20. All specified authorities subject to the duty will need to ensure they provide appropriate training for staff involved in the implementation of this duty. Such training is now widely available.

Sharing information

21. The *Prevent* programme must not involve any covert activity against people or communities. But specified authorities may need to share personal information to ensure, for example, that a person at risk of radicalisation is given appropriate support (for example on the Channel programme). Information sharing must be assessed on a case-by-case basis and is

governed by legislation. To ensure the rights of individuals are fully protected, it is important that information sharing agreements are in place at a local level. When considering sharing personal information, the specified authority should take account of the following:

- necessity and proportionality: personal information should only be shared where it is strictly necessary to the intended outcome and proportionate to it. Key to determining the necessity and proportionality of sharing information will be the professional judgement of the risks to an individual or the public;
 - consent: wherever possible the consent of the person concerned should be obtained before sharing any information about them;
 - power to share: the sharing of data by public sector bodies requires the existence of a power to do so, in addition to satisfying the requirements of the Data Protection Act 1998 and the Human Rights Act 1998;
 - Data Protection Act and the Common Law Duty of Confidentiality: in engaging with non-public bodies, the specified authority should ensure that they are aware of their own responsibilities under the Data Protection Act and any confidentiality obligations that exist.
22. There may be some circumstances where specified authorities, in the course of *Prevent*-related work, identify someone who may already be engaged in illegal terrorist-related activity. People suspected of being involved in such activity must be referred to the police.

D. Monitoring and enforcement

23. All specified authorities must comply with this duty and will be expected to maintain appropriate records to show compliance with their responsibilities and provide reports when requested.

Central support and monitoring

24. The Home Office currently oversees *Prevent* activity in local areas which have been identified as priorities for this programme, and will provide central monitoring for the new duty. The Home Office shares management (with local authorities) of local *Prevent* co-ordinator teams.

25. The Home Office will:

- draw together data about implementation of *Prevent* from local and regional *Prevent* co-ordinators (including those in health, further and higher education), the police, intelligence agencies and other departments and inspection bodies where appropriate;
- monitor and assess *Prevent* delivery in up to 50 *Prevent* priority areas;
- maintain contact with relevant departments and escalate issues to them and inspectorates where appropriate;
- support the *Prevent* Oversight Board, chaired by the Minister for Immigration and Security, which may agree on further action to support implementation of the duty.

26. Where a specified body is not complying with the duty, the *Prevent* Oversight Board may recommend that the Secretary of State use the power of direction under section 30 of the Act. This power would only be used when other options for engagement and improvement had been exhausted. The power would be used only to ensure the implementation and delivery of the *Prevent* duty. It is also capable of being exercised in respect of Welsh specified authorities, and would be used following consultation with Welsh Ministers.

Inspection regime in individual sectors

27. Central support and monitoring will be supported by existing inspection regimes in specific sectors. Not every specified authority has a suitable inspection regime and in some areas it may be necessary to create or enhance existing regimes.

28. We will work with the Welsh Government on *Prevent* monitoring arrangements and provide support to Welsh inspection regimes as required.

E. Sector-specific guidance

Local authorities

29. With their wide-ranging responsibilities, and democratic accountability to their electorate, local authorities are vital to *Prevent* work. Effective local authorities will be working with their local partners to protect the public, prevent crime and to promote strong, integrated communities.

Specified local authorities

30. The local authorities that are subject to the duty are listed in Schedule 6 to the Act. They are:

- a county council or district council in England;
- the Greater London Authority;
- a London borough council;
- the Common Council of the City of London in its capacity as a local authority;
- the Council of the Isles of Scilly;
- a county council or county borough council in Wales; and
- a person carrying out a function of an authority mentioned in section 1 (2) of the Local Government Act 1999 by virtue of a direction made under section 15 of that Act.

31. Other local authorities, including stand-alone fire and rescue authorities, are not listed in the Act and are not subject to the duty, but it is anticipated, considering their wider prevention role, that in many areas they will be partners in local efforts to prevent people from being drawn into terrorism.

32. In fulfilling the new duty, local authorities, including elected members and senior officers should be carrying out activity in the following areas.

Partnership

33. Local authorities should establish or make use of an existing local multi-agency group to agree risk and co-ordinate *Prevent* activity.

Many local authorities use Community Safety Partnerships but other multi-agency forums may be appropriate.

34. It is likely that links will need to be made to other statutory partnerships such as Local Safeguarding Children Boards Safeguarding Adults Boards, Channel panels and Youth Offending Teams.

35. It will be important that local or regional *Prevent* co-ordinators have access to senior local authority leadership to give advice and support.

36. We expect local multi-agency arrangements to be put in place to effectively monitor the impact of *Prevent* work.

37. *Prevent* work conducted through local authorities will often directly involve, as well as have an impact on local communities. Effective dialogue and coordination with community-based organisations will continue to be essential.

Risk assessment

38. We expect local authorities to use the existing counter-terrorism local profiles (CTLPs), produced for every region by the police, to assess the risk of individuals being drawn into terrorism. This includes not just violent extremism but also non-violent extremism, which can create an atmosphere conducive to terrorism and can popularise views which terrorists exploit. Guidance on CTLPs is available here:

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/118203/counter-terrorism-local-profiles.pdf

39. This risk assessment should also be informed by engagement with *Prevent* co-ordinators, schools, registered childcare providers, universities, colleges, local prisons, probation services, health, immigration enforcement Youth Offending Teams and others, as well as by a local authority's own knowledge of its area.

40. We would expect local authorities to incorporate the duty into existing policies and procedures, so it becomes part of the day-to-day work of the authority. The duty is likely to be relevant to fulfilling safeguarding responsibilities in that local authorities should ensure that there are clear and robust safeguarding policies to identify children at risk. This guidance should be read in conjunction with other relevant safeguarding guidance, in particular Working Together to Safeguard Children (<https://www.gov.uk/government/publications/working-together-to-safeguard-children>).

Action plan

41. With the support of co-ordinators and others as necessary, any local authority that assesses, through the multi-agency group, that there is a risk should develop a Prevent action plan. This will enable the local authority to comply with the duty and address whatever risks have been identified.

42. These local action plans will identify, prioritise and facilitate delivery of projects, activities or specific interventions to reduce the risk of people being drawn into terrorism in each local authority. Many of these projects and activities will be community based.

Staff training

43. Local authorities will be expected to ensure appropriate frontline staff, including those of it's contractors, have a good understanding of Prevent are trained to recognise vulnerability to being drawn into terrorism and are aware of available programmes to deal with this issue.

44. Local authority staff will be expected to make appropriate referrals to Channel (a programme which provides support to individuals who are at risk of being drawn into terrorism which is put on a statutory footing by Chapter 2 of Part 5 of the Counter-Terrorism and Security Act 2015) and ensure that Channel is supported by the appropriate organisation and expertise. Guidance on the Channel programme can be found here:

<https://www.gov.uk/government/publications/channel-guidance>

Use of local authority resources

45. In complying with the duty we expect local authorities to ensure that publicly-owned venues and resources do not provide a platform for extremists and are not used to disseminate extremist views. This includes considering whether IT equipment available to the general public should use filtering solutions that limit access to terrorist and extremist material.

46. We expect local authorities to ensure that organisations who work with the local authority on Prevent are not engaged in any extremist activity or espouse extremist views.

47. Where appropriate, we also expect local authorities to take the opportunity when new contracts for the delivery of their services are being made to ensure that the principles of the duty are written in to those contracts in a suitable form.

Collaboration between areas

48. In two-tier areas, county and district councils will need to agree proportionate arrangements for sharing the assessment of risk and for agreeing local *Prevent* action plans. It is expected that neighbouring areas will also agree proportionate arrangements for sharing the assessment of risk and for agreeing local *Prevent* action plans as appropriate.

Prevent priority areas

49. The Home Office will continue to identify priority areas for *Prevent*-related activity. Priority areas will, as now, be funded to employ a local *Prevent* co-ordinator to give additional support and expertise and additional Home Office grant funding is available for *Prevent* projects and activities. The Home Office will continue to have oversight of local *Prevent* co-ordinators and the funding, evaluation and monitoring of these projects.

Other agencies and organisations supporting children

50. A range of private and voluntary agencies and organisations provide services or, in some cases, exercise functions in relation to children. The duty applies to those bodies, which include, for example, children's homes and independent fostering agencies and bodies exercising local authority functions whether under voluntary delegation arrangements or via the use of statutory intervention powers. These bodies should ensure they are part of their local authorities' safeguarding arrangements and that staff are aware of and know how to contribute to *Prevent*-related activity in their area where appropriate.

Out-of-school settings supporting children

51. Many children attend a range of out-of-school settings other than childcare including supplementary schools, and tuition centres to support home education. These settings are not regulated under education law. Local authorities should take steps to understand the range of activity and settings in their areas and take appropriate and proportionate steps to ensure that children attending such settings are properly safeguarded (which should include considering whether children attending such settings are at risk of being drawn into extremism or terrorism). In assessing the risks associated with such settings, local authorities should have regard to whether the settings subscribe to voluntary accreditation schemes and any other evidence about the extent to which the providers are taking steps to safeguard the children in their care. Where safeguarding concerns arise, local authorities should actively consider how to make use of the full range of powers available to them to reduce the risks to children, including relevant planning and health and safety powers.

Monitoring and enforcement

52. In fulfilling its central monitoring role (section D above) the Home Office can (and already does) scrutinise local *Prevent* action plans, project impact and overall performance. It will also consider work with local authority 'peers' to provide targeted assistance and help authorities develop good practice.

53. The Government anticipates that local authorities will comply with this duty and work effectively with local partners to prevent people from being drawn into terrorism. Where there are concerns about compliance, the Government may need to consider the appropriateness of using existing mechanisms such as section 10 of the Local Government Act 1999. This allows the Secretary of State to appoint an inspector to assess an authority's compliance with its statutory "best value" duty in relation to one or more of the specified functions.

54. If the Secretary of State is satisfied that a council in England has failed to discharge its "best value" duty in relation to the new *Prevent* duty, it would be open to him to use his powers under Section 15 of the Local Government Act 1999 to intervene. This could include requiring the council to undertake specific actions, appointing Commissioners and transferring some of the council's functions to them. The Secretary of State must consult the council before issuing a direction. The Secretary of State may also direct a local inquiry to be held into the exercise by the authority of specified functions. Welsh Ministers' powers of intervention in relation to a Welsh council that has failed to discharge its "improvement" duties are set out in the Local Government (Wales) Measure 2009.

55. If the Secretary of State is satisfied that a local authority is failing to perform any function relating to education, childcare or children's social care to an adequate standard he may use his powers under section 497A or the Education Act 1996 (applied to childcare under section

15(3) of the Children's Act, and children's social care under section 50(1) of the Children Act 2004) to take whatever action is deemed expedient to achieve necessary improvement. In Wales, Welsh Ministers have the power to intervene under the School Standards and Organisation (Wales) Act 2013. These intervention measures are considered in cases where Ofsted inspections (or Estyn in Wales) identify inadequate practice and serious concerns about practice in relation to safeguarding, adoption and looked-after children. The Care and Social Services Inspectorate Wales (CSSIW) has a role here in terms of care settings and standards.

56. In addition to the powers above, the Act provides the Secretary of State with the power to issue a direction where a local authority has failed to discharge the duty (see paragraph 26, above).

Schools and registered childcare providers (excluding higher and further education).

57. In England about eight million children are educated in some 23,000 publicly-funded and around 2,400 independent schools. The publicly-funded English school system comprises maintained schools (funded by local authorities), and academies (directly funded by central government). In Wales, over 450,000 children attend Local Authority maintained schools, and there are 70 independent schools.¹

58. All publicly-funded schools in England are required by law to teach a broad and balanced curriculum which promotes the spiritual, moral, cultural, mental and physical development of pupils and prepares them for the opportunities, responsibilities and experiences of life. They must also promote community cohesion. Independent schools set their own curriculum but must comply with the Independent School Standards, which include an explicit requirement to promote fundamental British values as part of broader requirements relating to the quality of education and to promoting the spiritual, moral, social and cultural development of pupils. These standards also apply to academies (other than 16-19 academies), including free schools, as they are independent schools. 16-19 academies may have these standards imposed on them by the provisions of their funding agreement with the Secretary of State.

59. In Wales, independent schools set their own curriculum, but must comply with Independent Schools Standards made by the Welsh Ministers. These Standards also include a requirement to promote the spiritual, moral, social and cultural development of pupils.

60. Early years providers serve arguably the most vulnerable and impressionable members of society. The Early Years Foundation Stage (EYFS) accordingly places clear duties on providers to

keep children safe and promote their welfare. It makes clear that to protect children in their care, providers must be alert to any safeguarding and child protection issues in the child's life at home or elsewhere (paragraph 3.4 EYFS). Early years providers must take action to protect children from harm and should be alert to harmful behaviour by other adults in the child's life.

61. Early years providers already focus on children's personal, social and emotional development. The Early Years Foundation Stage framework supports early years providers to do this in an age appropriate way, through ensuring children learn right from wrong, mix and share with other children and value other's views, know about similarities and differences between themselves and others, and challenge negative attitudes and stereotypes.

62. This guidance should be read in conjunction with other relevant guidance. In England, this includes Working Together to Safeguard Children, Keeping Children Safe in Education and Information Sharing: Her Majesty's Government advice for professionals providing safeguarding services to children, young people, parents and carers.

<https://www.gov.uk/government/publications/working-together-to-safeguard-children>;

<https://www.gov.uk/government/publications/keeping-children-safe-in-education>;

63. In Wales it should be read alongside Keeping learners safe²:

<http://wales.gov.uk/docs/dcells/publications/150114-keeping-learners-safe.pdf>.

64. The authorities specified in paragraph 65 below are subject to the duty to have due regard to the need to prevent people from being drawn into terrorism. Being drawn into terrorism includes not just violent extremism but also non-violent extremism, which can create an

¹ Schools Census results on Wales.gov.uk

² Keeping Learners Safe includes advice on radicalisation on page 51

atmosphere conducive to terrorism and can popularise views which terrorists exploit. Schools should be safe spaces in which children and young people can understand and discuss sensitive topics, including terrorism and the extremist ideas that are part of terrorist ideology, and learn how to challenge these ideas. The Prevent duty is not intended to limit discussion of these issues. Schools should, however, be mindful of their existing duties to forbid political indoctrination and secure a balanced presentation of political issues. These duties are imposed on maintained schools by sections 406 and 407 of the Education Act 1996. Similar duties are placed on the proprietors of independent schools, including academies (but not 16-19 academies) by the Independent School Standards.

Education and childcare specified authorities

65. The education and childcare specified authorities in Schedule 6 to the Act are as follows:

- the proprietors³ of maintained schools, non-maintained special schools, maintained nursery schools, independent schools (including academies and free schools) and alternative provision academies⁴
- pupil referral units
- registered early years childcare providers⁵
- registered later years childcare providers⁶
- providers of holiday schemes for disabled children
- persons exercising local authority functions under a direction of the Secretary of State when the local authority is performing inadequately; and
- persons authorised by virtue of an order made under section 70 of the Deregulation and Contracting Out Act 1994 to exercise a function specified in Schedule 36A to the Education Act 1996.

66. In fulfilling the new duty, we would expect the specified authorities listed above to demonstrate activity in the following areas.

Risk assessment

67. Specified authorities are expected to assess the risk of children being drawn into terrorism, including support for extremist ideas that are part of terrorist ideology. This should be based on an understanding, shared with partners, of the potential risk in the local area.

68. Specified authorities will need to demonstrate that they are protecting children and young people from being drawn into terrorism by having robust safeguarding policies in place to identify children at risk, and intervening as appropriate. Institutions will need to consider the level of risk to identify the most appropriate referral, which could include Channel or Children's Social Care, for example. These policies should set out clear protocols for ensuring that any visiting speakers – whether invited by staff or by children themselves – are suitable and appropriately supervised.

Working in partnership

69. In England, governing bodies and proprietors of all schools and registered childcare providers should ensure that their safeguarding arrangements take into account the policies and procedures of the Local Safeguarding Children Board (LSCB). In Wales, Local Service Boards provide strategic oversight.

³ Reference in this guidance to the 'proprietor' in the case of a maintained school, maintained nursery school and non-maintained special school is a reference to the governing body of the school.

⁴ Including early years and later years childcare provision in schools that is exempt from registration under the Childcare Act 2006

⁵ Those registered under Chapter 2 or 2a of Part 3 of the Childcare Act 2006, including childminders

⁶ Those registered under Chapter 3 or 2a of Part 3 of the Childcare Act 2006, including childminders

Staff training

70. Specified authorities should make sure that staff have training that gives them the knowledge and confidence to identify children at risk of being drawn into terrorism, and to challenge extremist ideas which can be used to legitimise terrorism and are shared by terrorist groups. They should know where and how to refer children and young people for further help. Prevent awareness training will be a key part of this.

IT policies

71. Specified authorities will be expected to ensure children are safe from terrorist and extremist material when accessing the internet in school, including by establishing appropriate levels of filtering.

Monitoring and enforcement

72. The Office for Standards in Education, Children's Services and Skills (Ofsted) inspects the specified authorities in England listed above, with the exception of some privately funded independent schools. When assessing the effectiveness of schools, Ofsted inspectors already have regard to the school's approach to keeping pupils safe from the dangers of radicalisation and extremism, and what is done when it is suspected that pupils are vulnerable to these. Maintained schools are subject to intervention, and academies and free schools may be subject to termination of their funding agreement, if they are judged by Ofsted to require significant improvement or special measures, or if they fail to take the steps required by their local authority, or for academies or free schools by the Secretary of State pursuant to their funding agreement, as applicable, to address unacceptably low standards, serious breakdowns of management or governance or if the safety of pupils or staff is threatened. In Wales, all publicly funded schools are inspected by Estyn.

73. Ofsted inspects 16-19 academies under the Common Inspection Framework for further education and skills.

74. Privately funded independent schools in England are inspected by Ofsted or one of three independent inspectorates. In Wales, Estyn inspects independent schools. If they fail to meet the Independent School Standards, they must remedy the problem or be subject to regulatory action by the Department for Education or the Welsh Government, which could include de-registration (which would make their continued operation unlawful).

75. Early education funding regulations in England have been amended to ensure that providers who fail to promote the fundamental British values of democracy, the rule of law, individual liberty and mutual respect and tolerance for those with different faiths and beliefs do not receive funding from local authorities for the free early years entitlement.

76. Ofsted's current inspection framework for early years provision reflects the requirements in the Statutory Framework for the Early Years Foundation Stage.

Further education

77. There is an important role for further education institutions, including sixth form colleges and independent training providers, in helping prevent people being drawn into terrorism, which includes not just violent extremism but also non-violent extremism, which can create an atmosphere conducive to terrorism and can popularise views which terrorists exploit. It is a condition of funding that all further education and independent training providers must comply with relevant legislation and any statutory responsibilities associated with the delivery of education and safeguarding of learners.

78. There will be further guidance issued on the management of external speakers and events, including on the interaction of the Prevent duty with institutions' existing duty to secure freedom of speech.

79. But it is important to realise that the risk of radicalisation in institutions does not just come from external speakers. Radicalised students can also act as a focal point for further radicalisation through personal contact with fellow students and through their social media activity. Where radicalisation happens off campus, the student concerned may well share his or her issues with other students. Changes in behaviour and outlook may be visible to staff. Much of this section therefore addresses the need for institutions in receipt of public funding to self assess and identify the level of risk, ensure all staff have access to training, and that there is welfare support for students and effective IT policies in place which ensure that these signs can be recognised and responded to appropriately.

Further education specified authorities

80. The further education specified in Schedule 6 to the Act fall into the following categories:

- further education institutions on the Skills Funding Agency (SFA) register of training organisations (ROTO), including sub-contractors which receive more than £100,000 of SFA funding via lead providers. This includes

approximately 950 further education colleges and independent providers – such as private companies and third sector organisations that are eligible to receive public funding from the SFA to deliver education and training and the 93 Sixth Form Colleges and other organisations funded by the Education Funding Agency to deliver post 16 education and training;

- further education institutions in Wales funded by the Welsh Government; and
- private further education institutions who are not in receipt of public funding who may be on the UK Register of Learning Providers and have similar characteristics to those on the register. We define these as institutions that have at least 250 students who are undertaking courses in preparation for examinations which either receive public funding or are regulated by the Office of Qualifications and Examinations Regulation or the Welsh Government.

81. Most institutions already understand their *Prevent*-related responsibilities, especially in the context of ensuring the welfare of learners, staff and visitors, and there are numerous examples of good practice in these areas. As with higher education (see below), compliance with this duty will reflect existing best practice and should not add significant new burdens on institutions. It is to be implemented in a proportionate and risk-based way.

82. To comply with the duty we would expect further education institutions to be delivering in the following ways.

Partnership

83. In complying with this duty we would expect active engagement from governors, boards, principals, managers and leaders with other partners including police and BIS regional higher and further education *Prevent* co-ordinators (details of BIS *Prevent* co-ordinators can be found at www.safecampuscommunities.ac.uk). We would expect institutions to seek to engage and consult students on their plans for implementing the duty.

84. Where the size of an institution warrants, management and co-ordination arrangements should be implemented to share information across the relevant curriculum areas within an institution, with a single point of contact for operational delivery of Prevent-related activity.

Risk assessment

85. Each institution should carry out a risk assessment which assesses where and how students or staff may be at risk of being drawn into terrorism. These policies and procedures will help an institution satisfy itself and government that it is able to identify and support these individuals.

86. We would expect the risk assessment to look at institutional policies regarding the campus and student welfare, including equality and diversity, and the safety and welfare of students and staff. We expect the risk assessment to address the physical management of the institution's estate, including policies and procedures for events held by staff, students or visitors, and relationships with external bodies and community groups who may use premises, or work in partnership with the institution.

87. Institutions must have clear and visible policies and procedures for managing whistle-blowing and complaints. In England, if an individual feels that their complaint has *not* been taken seriously by the college or provider they can raise it with the SFA (for Further Education and Private Providers) or EFA (for sixth form colleges or private providers funded by it).

88. Where an institution has sub-contracted the delivery of courses to other providers, we expect robust procedures to be in place to ensure that the sub-contractor is aware of the Prevent duty and the sub-contractor is not inadvertently funding extremist organisations.

89. In Wales the Safer Working Practice Guidance and assessment process should also be adhered to.

Action Plan

90. Any institution that identifies a risk should notify the relevant BIS *Prevent* co-ordinator and others as necessary (such as the SFA, EFA Welsh Government and the police) and develop a Prevent action plan to set out the actions they will take to mitigate the risks.

Staff Training

91. We would expect institutions to demonstrate that it undertakes appropriate training and development for principals, governors, leaders and staff. This will enable teachers and others supporting delivery of the curriculum to use opportunities in learning to educate and challenge. It will also allow leaders and teachers to exemplify British values in their management, teaching and through general behaviours in institutions, including through opportunities in the further education curriculum. We expect institutions to encourage students to respect other people with particular regard to the protected characteristics set out in the Equality Act 2010.

92. We would expect appropriate members of staff to have an understanding of the factors that make people vulnerable to being drawn into terrorism and to challenge extremist ideas which are used by terrorist groups and can purport to legitimise terrorist activity. We define extremism as "vocal or active opposition to fundamental British values, including democracy, the rule of law, individual liberty and mutual respect and tolerance for those with different faiths and beliefs. We also include in our definition of extremism calls for the death of members of our armed forces, whether in this country or overseas." Such staff should have sufficient training to be able to recognise this vulnerability and be aware of what action to take in response. This will include an understanding of when to make referrals to the Channel programme and where to get additional advice and support.

93. At a corporate level we would expect the institution to have robust procedures both internally and externally for sharing information about vulnerable individuals. This should include information sharing agreements where possible.

94. As the independent body responsible for standards and quality improvement for further education, the Education and Training Foundation will work with the sector to ensure that appropriate training is available. This will include and draw from training provided through the network of Prevent co-ordinators.

Welfare and pastoral care/chaplaincy support

95. All institutions have a clear role to play in the welfare of their students and we would expect that there to be sufficient pastoral care and support available for all students.

96. As part of this, we would expect the institution to have clear and widely available policies for the use of prayer rooms and other faith-related facilities. These policies should outline structures in place for the managing prayer and faith facilities (for example an oversight committee) and mechanisms for managing any issues arising from the use of the facilities.

IT policies

97. We would expect institutions to have policies relating to the use of their IT equipment. Whilst all institutions will have policies around general usage, covering what is and is not permissible, we would expect that all policies and procedures will contain specific reference to the duty. Many educational institutions already use filtering as a means of restricting access to harmful content, and should consider the use of filters as part of their overall strategy to prevent people from being drawn into terrorism.

98. Institutions must have clear policies in place for students and staff using IT equipment to research terrorism and counter terrorism in the course of their learning.

99. The Joint Information Systems Committee (JISC) can provide specialist advice and support to the FE sector in England to help providers ensure students are safe online and appropriate safeguards are in place. JISC also has a Computer Security Incident Response Team who can provide assistance in the event of an online incident occurring.

Monitoring and enforcement

100. Ofsted inspects publicly funded further education and skills providers in England under the Common Inspection Framework. This inspection is risk-based and the frequency with which providers are inspected depends on this risk. Safeguarding is inspected as part of leadership and management judgement. In Wales the inspection regime is operated by Estyn.

101. Where Ofsted finds a publicly-funded further education institution or independent training provider inadequate intervention action would be taken. In the case of independent providers this is likely to result in their contract being terminated by the Skills Funding Agency. In the case of further education institutions and local authority providers, this would result in the Further Education or Sixth Form College Commissioner making an immediate assessment. This could lead to governance and leadership change, restructuring or even dissolution under the Secretary of State's reserve powers. Under the Further and Higher Education Act 1992 Act, and following intervention action, it would also be possible for the Secretary of State to issue a direction as the ultimate sanction.

102. For those institutions that are not publicly funded, the Secretary of State will have a power to nominate a body to monitor compliance with the duty and undertake risk-based assessments.

Higher education

103. Universities' commitment to freedom of speech and the rationality underpinning the advancement of knowledge means that they represent one of our most important arenas for challenging extremist views and ideologies. But young people continue to make up a disproportionately high number of those arrested in this country for terrorist-related offences and of those who are travelling to join terrorist organisations in Syria and Iraq. Universities must be vigilant and aware of the risks this poses.

104. Some students may arrive at universities already committed to terrorism; others may become radicalised whilst attending university due to activity on campus; others may be radicalised whilst they are at university but because of activities which mainly take place off campus.

105. Radicalisation on campus can be facilitated through events held for extremist speakers. There will be further guidance issued on the management of external speakers and events, including on the interaction of the *Prevent* duty with universities' existing duties to secure freedom of speech and have regard to the importance of academic freedom.

106. But managing the risk of radicalisation in universities is not simply about managing external speakers. Radicalised students can also act as a focal point for further radicalisation through personal contact with fellow students and through their social media activity. Where radicalisation happens off campus, the student concerned may well share his or her issues with other students. Changes in behaviour and outlook may be visible to university staff. Much of this section addresses the need for universities to have the necessary staff training, IT policies and student welfare programmes to recognise these signs and respond appropriately.

Higher education specified authorities

107. The higher education institutions specified in Schedule 6 to the Act fall into two categories:

- the governing body of qualifying institutions within the meaning given by section 11 of the Higher Education Act 2004.
- private higher education institutions that are not in receipt of public funding from the Higher Education Funding Council for England (HEFCE) or the Higher Education Funding Council Wales (HEFCW) but have similar characteristics to those that are. This includes governing bodies or proprietors of institutions not otherwise listed that have at least 250 students, excluding students on distance learning courses, undertaking courses of a description mentioned in Schedule 6 to the Education Reform Act 1988 (higher education courses).

108. Most of these institutions already have a clear understanding of their *Prevent* related responsibilities. Institutions already demonstrate some good practice in these areas. We do not envisage the new duty creating large new burdens on institutions and intend it to be implemented in a proportionate and risk-based way.

109. Compliance with the *Prevent* duty requires that properly thought through procedures and policies are in place. Having procedures and policies in place which match the general expectations set out in this guidance will mean that institutions are well placed to comply with the *Prevent* duty. Compliance will only be achieved if these procedures and policies are properly followed and applied. This guidance does not prescribe what appropriate decisions would be - this will be up to institutions to determine, having considered all the factors of the case.

110. We would expect universities and higher education institutions to be delivering in the following areas.

Partnership

111. In complying with this duty we would expect active engagement from senior management of the university (including, where appropriate, vice chancellors) with other partners including police and BIS regional higher and further education

Prevent co-ordinators. We would expect institutions to seek to engage and consult students on their plans for implementing the duty.

112. Given the size and complexity of most institutions we would also expect universities to make use of internal mechanisms to share information about *Prevent* across the relevant faculties of the institution. Having a single point of contact for operational delivery of *Prevent*-related activity may also be useful.

113. We would expect institutions to have regular contact with the relevant *Prevent* co-ordinator. These co-ordinators will help universities comply with the duty and can provide advice and guidance on risk and on the appropriate response. The contact details of these co-ordinators are available on the Safe Campus Communities website: www.safecampuscommunities.ac.uk.

Risk assessment

114. Universities will be expected to carry out a risk assessment for their institution which assesses where and how their students might be at risk of being drawn into terrorism. This includes not just violent extremism but also non-violent extremism, which can create an atmosphere conducive to terrorism and can popularise views which terrorists exploit. Help and support will be available to do this.

115. We would expect the risk assessment to look at institutional policies regarding the campus and student welfare, including equality and diversity and the safety and welfare of students and staff. We would also expect the risk assessment to assess the physical management of the university estate including policies and procedures for events held by staff, students or visitors and relationships with external bodies and community groups who may use premises, or work in partnership with the institution.

Action Plan

116. With the support of co-ordinators, and others as necessary, any institution that identifies a risk should develop a *Prevent* action plan to institution to set out the actions they will take to mitigate this risk.

Staff Training

117. Compliance with the duty will also require the institution to demonstrate that it is willing to undertake *Prevent* awareness training and other training that could help the relevant staff prevent people from being drawn into terrorism and challenge extremist ideas which risk drawing people into terrorism. We would expect appropriate members of staff to have an understanding of the factors that make people support terrorist ideologies or engage in terrorist-related activity. Such staff should have sufficient training to be able to recognise vulnerability to being drawn into terrorism, and be aware of what action to take to take in response. This will include an understanding of when to make referrals to the Channel programme and where to get additional advice and support.

118. We would expect the institution to have robust procedures both internally and externally for sharing information about vulnerable individuals (where appropriate to do so). This should include appropriate internal mechanisms and external information sharing agreements where possible.

119. BIS offers free training for higher and further education staff through its network of regional higher and further education *Prevent* co-ordinators. This covers safeguarding and identifying vulnerability to being drawn into terrorism and can be tailored to suit each institution or group of individuals

Welfare and pastoral care/chaplaincy support

120. Universities have a clear role to play in the welfare of their students and we would expect there to be sufficient chaplaincy and pastoral support available for all students.

21. As part of this, we would expect the institution to have clear and widely available policies for the use of prayer rooms and other faith-related facilities. These policies should outline arrangements for managing prayer and faith facilities (for example an oversight committee) and for dealing with any issues arising from the use of the facilities.

IT policies

122. We would expect universities to have policies relating to the use of university IT equipment. Whilst all institutions will have policies around general usage, covering what is and is not permissible, we would expect these policies to contain specific reference to the statutory duty. Many educational institutions already use filtering as a means of restricting access to harmful content, and should consider the use of filters as part of their overall strategy to prevent people from being drawn into terrorism.

123. To enable the university to identify and address issues where online materials are accessed for non-research purposes, we would expect to see clear policies and procedures for students and staff working on sensitive or extremism-related research. Universities UK has provided guidance to help universities manage this, which available at

[http://www.universitiesuk.ac.uk/highereducation/Pages/Oversight Of SecuritySensitiveResearch Material.aspx](http://www.universitiesuk.ac.uk/highereducation/Pages/Oversight%20Of%20SecuritySensitiveResearchMaterial.aspx)

Student unions and societies

124. Institutions should have regard to the duty in the context of their relationship and interactions with student unions and societies. They will need to have clear policies setting out the activities that are or are not allowed to take place on campus and any online activity directly related to the university. The policies should set out what is expected from the student unions and societies in relation to *Prevent* including making clear the need to challenge extremist ideas which risk drawing people into terrorism. We would expect student unions and societies to work closely with their institution and co-operate with the institutions' policies.

125. Student unions, as charitable bodies, are registered with the Charity Commission and subject to charity laws and regulations, including those that relating to preventing terrorism. Student Unions should also consider whether their staff and elected officers would benefit from *Prevent* awareness training or other relevant training provided by the Charity Commission, regional *Prevent* co-ordinators or others.

Monitoring and enforcement

126. The Secretary of State will appoint an appropriate body to assess the bodies' compliance with the *Prevent* duty. A separate monitoring framework will be published setting out the details of how this body will undertake monitoring of the duty.

The health sector

127. Healthcare professionals will meet and treat people who may be vulnerable to being drawn into terrorism. Being drawn into terrorism includes not just violent extremism but also non-violent extremism, which can create an atmosphere conducive to terrorism and can popularise views which terrorists exploit.

128. The key challenge for the healthcare sector is to ensure that, where there are signs that someone has been or is being drawn into terrorism, the healthcare worker is trained to recognise those signs correctly and is aware of and can locate available support, including the Channel programme where necessary. Preventing someone from being drawn into terrorism is substantially comparable to safeguarding in other areas, including child abuse or domestic violence.

129. There are already established arrangements in place, which we would expect to be built on in response to the statutory duty.

Health specified authorities

130. The health specified authorities in Schedule 6 to the Act are as follows:

- NHS Trusts
- NHS Foundation Trusts

131. NHS England has incorporated *Prevent* into its safeguarding arrangements, so that *Prevent* awareness and other relevant training is delivered to all staff who provide services to NHS patients. These arrangements have been effective and should continue.

132. The Chief Nursing Officer in NHS England has responsibility for all safeguarding, and a safeguarding lead, working to the Director of Nursing, is responsible for the overview and management of embedding the *Prevent* programme into safeguarding procedures across the NHS.

133. Each regional team in the NHS has a Head of Patient Experience who leads on safeguarding in their region. They are responsible for delivery

of the *Prevent* strategy within their region and the health regional *Prevent* co-ordinators (RPCs).

134. These RPCs are expected to have regular contact with *Prevent* leads in NHS organisations to offer advice and guidance.

135. In Wales, NHS Trusts and Health Boards have CONTEST *Prevent* leads and part of multi-agency structures where these are in place. This guidance should be read in conjunction with *Building Partnerships-Staying Safe* issued by the Department of Health and Social Services, which provides advice to healthcare organisations on their role in preventing radicalisation of vulnerable people as part of their safeguarding responsibilities.

136. In fulfilling the duty, we would expect health bodies to demonstrate effective action in the following areas.

Partnership

137. All Sub Regions within the NHS should, under the NHS England Accountability and Assurance Framework, have in place local Safeguarding Forums, including local commissioners and providers of NHS Services. These forums have oversight of compliance with the duty, and ensure effective delivery. Within each area, the RPCs are responsible for promoting *Prevent* to providers and commissioners of NHS services, supporting organisations to embed *Prevent* into their policies and procedures, and delivering training.

138. We would expect there to be mechanisms for reporting issues to the National *Prevent* sub board.

139. We would also expect the *Prevent* lead to have networks in place for their own advice and support to make referrals to the Channel programme.

140. Since April 2013 commissioners have used the NHS Standard Contract for all commissioned services excluding Primary Care, including private and voluntary organisations. Since that time, the Safeguarding section of the contract

has required providers to embed *Prevent* into their delivery of services, policies and training. This should now be bolstered by the statutory duty.

Risk Assessment

141. All NHS Trusts in England have a *Prevent* lead who acts as a single point of contact for the health regional *Prevent* co-ordinators, and is responsible for implementing *Prevent* within their organisation. To comply with the duty, staff are expected, as a result of their training, to recognise and refer those at risk of being drawn into terrorism to the *Prevent* lead who may make a referral to the Channel programme. Regional health *Prevent* co-ordinators are able to provide advice and support to staff as required. In Wales, Health is a member of the Wales Contest Board and similar arrangements are in place.

Staff Training

142. The intercollegiate guidance, *Safeguarding Children and Young people: roles and competences for health care staff* includes *Prevent* information and identifies competencies for all healthcare staff against six levels.

143. The training should allow all relevant staff to recognise vulnerability to being drawn into terrorism, (which includes someone with extremist ideas that are used to legitimise terrorism and are shared by terrorist groups), including extremist ideas which can be used to legitimise terrorism and are shared by terrorist groups, and be aware of what action to take in response, including local processes and policies that will enable them to make referrals to the Channel programme and how to receive additional advice and support.

144. It is important that staff understand how to balance patient confidentiality with the duty. They should also be made aware of the information sharing agreements in place for sharing information with other sectors, and get advice and support on confidentiality issues when responding to potential evidence that someone is being drawn into terrorism, either during informal contact or consultation and treatment.

145. We would therefore expect providers to have in place:

- Policies that include the principles of the *Prevent* NHS guidance and toolkit, which are set out in *Building Partnerships, Staying Safe: guidance for healthcare organisations*, which can be found here:

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/215253/dh_131912.pdf

- A programme to deliver *Prevent* training, resourced with accredited facilitators;
- Processes in place to ensure that using the intercollegiate guidance, staff receive *Prevent* awareness training appropriate to their role; and
- Procedures to comply with the *Prevent* Training and Competencies Framework.

Monitoring and enforcement

146. Within the NHS, we expect local safeguarding forums, including local commissioners and providers of NHS Services to have oversight of fulfilling the duty and ensuring effective delivery.

147. Externally, Monitor is the sector regulator for health services in England ensuring that independent NHS Foundation Trusts are well led so that they can provide quality care on a sustainable basis. The Trust Development Authority is responsible for overseeing the performance of NHS Trusts and the Care Quality Commission is the independent health and adult social care regulator that ensures these services provide people with safe, effective and high quality care. In Wales, the Healthcare Inspectorate Wales, and the Care and Social Services Inspectorate Wales could be considered to provide monitoring arrangements. We will work with the Welsh Government to consider the arrangements in Wales.

148. We are considering whether these internal arrangements are robust enough to effectively monitor compliance with the duty or whether the duty should be incorporated into the remit and inspection regimes of one of the existing health regulatory bodies, or another body.

Prisons and probation

149. As an executive agency of the Ministry of Justice, the National Offender Management Service (NOMS) is responsible for protecting the public and reducing re-offending through delivery of prison and probation services.

150. There are 122 prisons in England and Wales including 14 prisons operated under contract by private sector organisations. There are around 85,000 prisoners in custody at any one time and 150,000 individuals in custody during a 12 month period.

151. Probation services are delivered by the National Probation Service (NPS), which supervises high-risk and other serious offenders, and 21 Community Rehabilitation Companies (CRCs), which supervise low and medium-risk offenders. NOMS is currently responsible for around 220,000 offenders under probation supervision, subject either to community sentences or to licence conditions after release from custody.

152. This responsibility for public protection and reducing re-offending gives both prisons and probation services a clear and important role both in working with offenders convicted of terrorism or terrorism-related offences and in preventing other offenders from being drawn into terrorism and the extremist ideas that are used to legitimise terrorism and are shared by terrorist groups.

Criminal justice specified authorities

153. The criminal justice specified authorities listed in Schedule 6 to the Act are as follows:

- prisons and Young Offender Institutions (YOI), including those that are contracted out;
- the under-18 secure estate (under-18 YOI, Secure training centres and Secure care homes;
- secure training centres;
- the National Probation Service; and
- Community Rehabilitation Companies.

Prisons

154. NOMS manages the risk of offenders being drawn into, or reverting to, any form of offending as part of its core business (identifying and managing the risks presented by offenders).

155. To comply with the duty we would expect public and contracted out prisons to carry out activity in the following areas.

Preliminary risk assessment

156. Prisons should perform initial risk assessments on reception, including cell-sharing risk assessments, and initial reception and induction interviews to establish concerns in relation to any form of extremism, be that faith based, animal rights, environmental, far right, far left extremism or any new emerging trends.

157. Contact with prisons chaplaincy should take place, as an integral part of the induction process. Any concerns raised as a result of chaplaincy contact with prisoners, including any concerns about extremism, should be reported throughout the sentence.

158. Prisoners should have regular contact with trained staff who will report on behaviours of concern.

159. Appropriate information and intelligence sharing should take place, for example with law enforcement partners, to understand whether extremism is an issue and to identify and manage any behaviours of concern.

Assessing ongoing risk and interventions

160. For offenders convicted of terrorist or terrorist-related offences, mainstream offender management processes will be used to determine whether interventions are necessary. These are intended to challenge the index offence and can include, where appropriate, intervention disruption and relocation.

161. Where concerns around someone being drawn into terrorism (which includes someone with extremist ideas that are used to legitimise terrorism and are shared by terrorist groups) are identified, either during the early days in

custody or later, prison staff should report accordingly, through the intelligence reporting system. All such reporting should be regularly assessed by specialist staff in conjunction with the police.

162. Where such concerns are identified an establishment should look to support that individual. This could take the form of moving them away from a negative influence or providing them with mentoring from the relevant chaplain providing religious classes or guidance.

163. Management actions could also include a reduction in privilege level, anti-bullying intervention, adjudication or segregation. Alternatively, it may be appropriate to provide theological, motivational and behavioural interventions.

164. Intelligence and briefing packages targeted at staff working with terrorist and extremist prisoners and those at risk of being drawn into terrorism should continue to be made available and delivered. These should continue to be jointly delivered by appropriately trained prison staff and police, and will be updated as required. In complying with this duty, extremism awareness training provided to new staff should be increased.

Transition from custody to supervision in the community

165. Pre-release planning should take place for all prisoners, including those subject to sentences less than 12 months, who will now receive some level of post-release supervision. Prisons, probation providers and the police should consider what risks need to be managed in the community including those that have arisen whilst in custody and indicate a vulnerability to being drawn into terrorism. Where this is the case, a Channel referral will be considered as part of the risk management plans and a referral to Channel made at the earliest opportunity where appropriate.

166. For offenders already convicted of terrorism or terrorism-related offences, prisons will complete appropriate pre-release processes such as Multi-Agency Public Protection Arrangements (MAPPA) with relevant agencies including the police and the NPS. These processes ensure that the requirements of the duty are met in the management of terrorist offenders in the community with the NPS the lead agency in MAPPA for such cases.

167. For all prisoners, where sufficient remaining sentence time permits, a formal multi-agency meeting which includes the police and the probation counter terrorism lead, should take place to inform decisions after release. This will ensure that partner agencies work together to share relevant information and put provision in place to manage the risk or any outstanding concerns. This can apply to periods of Release on Temporary Licence, Home Detention Curfew as well as eventual release on licence.

168. Where insufficient time remains, police and probation staff should be given fast time briefing by prison counter-terrorism staff as above and the National Probation Service CT lead will ensure the probation provider in the community is aware of the information, the risks and relevant personnel within partner agencies.

Staff training

169. In complying with the duty, we would expect all new prison staff to receive Prevent awareness training (tailored specifically to the prison environment). For staff already in post, this should be provided through specialist training and briefing packages that cover working with extremist behaviour. This training can be delivered in partnership with the police and be available to those members of staff who work most closely with terrorist and identified extremist prisoners. All staff should have an understanding of general intelligence systems, reporting and procedures to enable them to report on extremist prisoners and those vulnerable to extremist messaging.

Under-18 secure estate

170. The under-18 secure estate differs in terms of governance and service provision to that of the prisons and probation services for adults.

171. The Youth Justice Board (YJB) has a statutory responsibility to commission secure services for children and young people under the age of 18 and has a statutory duty to place children and young people sentenced or remanded by the courts into secure establishments.

The under -18 secure estates consists of:

- **Secure Children's Homes (SCHs)**
Secure children's homes are run by local authority children's services, overseen by the Department of Health and the Department for Education. They have a high ratio of staff to young people and are generally small facilities, ranging in size from six to forty beds.
- **Secure Training Centres (STC)**
Secure training centres are purpose-built centres for young offenders up to and including the age of 17. They are run by private operators under contracts, which set out detailed operational requirements. There are currently three STCs in England.
- **Young Offender Institutions (YOI)**
Young offender institutions are facilities run by both the Prison Service and the private sector and can accommodate 15 to 21-year-old male offenders.

172. We would expect that staff at each secure estate and Youth Offending Teams (YOT) overseeing the care of the child or young person would receive appropriate training in identifying and managing those at risk of being drawn into terrorism.

173. As part of the ongoing care and monitoring of each child or young person, any indication of risk should be identified and a referral made to Channel if appropriate

Probation

174. To comply with the duty we would expect all providers of probation services, particularly the National Probation Service (NPS) and Community Rehabilitation Companies (CRCs) to demonstrate that they are delivering activities under all of the following categories.

Leadership

175. We would expect every NPS division to have a designated probation counter-terrorism lead (PCTL) to provide the leadership necessary at a regional level to ensure processes for identifying, assessing and managing high-risk terrorist offenders are followed. We would expect PCTLs to provide a consultative role to CRCs.

Partnerships

176. In all partnership working we would expect that all providers of probation services will comply with the duty; for example both the NPS and CRCs are partners in local Community Safety Partnerships (CSPs). Active participation in CSPs will enable all probation providers to work together with other partners to share information and develop joint referrals and interventions.

Risk assessment

177. We would expect probation staff to adopt an investigative stance in undertaking risk assessments as they should in all cases. Where there are concerns, albeit these may be intelligence led, about someone being at risk of being drawn into terrorism this should initially be recorded in the core risk assessment.

178. Additionally, we would expect existing risk assessment processes to be supplemented by specialist assessments, for example, extremism risk screening. We would expect PCTLs to provide a consultative role to CRCs in doing this, where appropriate.

179. For offenders already convicted of terrorist or terrorist-related offences we would expect the NPS to work in partnership with other agencies, including prisons and the police, to

manage any risks identified via MAPPA and to provide bespoke interventions where relevant. For offenders who have not been convicted of a terrorism-related offence and may not be MAPPA eligible, but who are subsequently at risk of being drawn into terrorism, we would expect probation providers to have processes in place to escalate these cases to other agencies or otherwise refer the offender for appropriate interventions – for example to the Channel programme.

Staff training

180. We would expect probation providers to ensure that all staff receive appropriate training in identifying and managing those at risk of being drawn into terrorism including those with extremist ideas that can be used to legitimise terrorism and are shared by terrorist groups. *Prevent* awareness training has already been given to probation staff in recent years. In complying with the duty, we expect this and other relevant *Prevent* training to continue.

181. In the future, we expect *Prevent* awareness training to be included within the Probation Qualification Framework, which is completed by all newly qualified probation staff in both the NPS and CRCs. In addition PCTLs should lead the development of, for example, faith awareness or Extremism Risk Screening training of local training and staff development to supplement the *Prevent* awareness training. This should focus on emerging issues and any new support and interventions that become available.

Monitoring and enforcement for prisons and probation

182. Within prisons, we would expect compliance with the duty to be monitored and enforced internally by:

- mandatory compliance with Prison Service Instructions and Orders which define policy and best practice; and
- regular assessment of levels and risk of extremism and radicalisation internally via regional counter-terrorism co-ordinators.

183. Externally, our preference is to use existing inspection regimes where appropriate to do so. We consider that a thematic inspection by HM Inspector of Prisons could be a useful addition to the monitoring arrangements outlined above.

184. For probation providers, internally, we would expect compliance with the duty to be reinforced by detailed operational guidance set out in Probation Instructions. CRCs are contractually required to comply with the mandatory actions in relevant Probation Instructions and a similar requirement exists for the NPS in Service Level Agreements. Compliance with Probation Instructions is monitored and assured internally by contract management and audit functions within NOMS and the Ministry of Justice

185. Externally, we consider that a thematic inspection by HM Inspector of Probation could be a useful addition to the monitoring arrangement outlined above.

186. The YJB monitors the flow of young people through the Youth Justice system identifying the needs and behaviours of young offenders working closely with local partners to improve the support available.

The police

187. The police play an essential role in most aspects of *Prevent* work alongside other agencies and partners. They hold information which can help assess the risk of radicalisation and disrupt people engaged in drawing others into terrorism (which includes not just violent extremism but also non-violent extremism, which can create an atmosphere conducive to terrorism and can popularise views which terrorists exploit). The Police work alongside other sectors in this document to play a galvanising role in developing local *Prevent* partnerships and bring together a wide range of other organisations to support local delivery of *Prevent*.

188. The police are uniquely placed to tackle terrorism and whilst it is acknowledged that the Police Service will designate dedicated *Prevent* roles within Policing, a key objective for the police is to ensure that *Prevent* is embedded into all aspects of policing including patrol, neighbourhood and safeguarding functions. In fulfilment of their duties consideration must be given to the use of all suitable police resources, not just those specifically designed as *Prevent*.

Police specified authorities

189. The police specified authorities listed in Schedule 6 to the Act are as follows:

- police forces in England and Wales;
- Police and Crime Commissioners;
- the British Transport Police;
- port police forces; and
- the Civil Nuclear Police Authority

190. In fulfilling the new duty we would expect the police to take action in the following areas.

Prosecute, disrupt and deter extremists

191. In complying with the duty, police should engage and where appropriate disrupt extremist activity, in partnership with other agencies. We expect the police to prioritise projects to

disrupt terrorist and extremist material on the internet and extremists working in this country. Officers should consider the full range of investigative and prosecution options when it comes to disrupting extremist behaviour, including the use of public order powers where appropriate. This may include:

- Enforcing terrorist proscription and public order legislation;
- Working with local authorities to consider municipal powers, including local highways and leafleting by-laws, using safeguarding of young people legislation;
- Advising other specified authorities, for example local authorities or universities, to develop venue booking processes and good practice;
- Lawfully disrupting or attending events involving extremist speakers in both private and municipal establishments;
- Providing high visibility police presence at relevant events in public places.

Supporting vulnerable individuals

192. *Prevent* requires a multi-agency approach to protect people at risk from radicalisation. When vulnerable individuals are identified the police will undertake the following:

- In partnership with other agencies including the local authority, consider appropriate interventions, including the Channel programme, to support vulnerable individuals;
- Work in partnership with and support Channel Panels chaired by local authorities to co-ordinate Channel partners and Channel actions;
- Support existing, and identify potential new Intervention Providers.

Partnership and risk assessment

193. The police should:

- Engage fully with the local multi-agency groups that will assess the risk of people being drawn into terrorism, providing (where appropriate) details of the police counter-terrorism local profile (CTLTP);
- Support the development and implementation by the multi agency group of a Prevent action plan to address that risk;
- Support local authority Prevent co-ordinators, regional further and higher education co-ordinators, regional health Prevent leads and regional NOMS Prevent co-ordinators in carrying out their work;
- Co-ordinate the delivery of the Channel programme by accepting referrals, including acting as a conduit for Channel referrals with partners; and
- Ensure Prevent considerations are fully embedded into counter-terrorism investigations.

194. The success of Prevent work relies on communities supporting efforts to prevent people being drawn into terrorism and challenging the extremist ideas that are also part of terrorist ideology. The police have a critical role in helping communities do this. To comply with the duty, we would expect the police, to support others including local authorities, to build community resilience by:

- Supporting local authority Prevent Coordinators in developing Prevent-related projects and action plans;

- Supporting the Charity Commission in providing guidance to avoid money being inadvertently given to organisations which may endorse extremism or terrorism and enforcing legislation where fraud offences are identified.
- Supporting opportunities to develop community challenges to extremists; and
- Collate and analyse community tension reporting across the UK that enables police and partners to identify and respond to emerging concerns.

Monitoring and enforcement

195. The Strategic Policing Requirement makes clear that Police and Crime Commissioners (PCCs) and Chief Constables must demonstrate that they have contributed to the government's counter terrorism strategy (CONTEST). This includes the Prevent programme, where they are required to take into account the need to identify and divert those involved in or vulnerable to radicalisation. The Home Secretary can direct a PCC to take specific action to address a specific failure.

196. HM Inspectorate of Constabulary (HMIC) is the statutory body for inspecting the police. They can carry out thematic inspections and can be asked to inspect a particular force or theme by the Home Secretary.

F. Glossary of terms

‘Having due regard’ means that the authorities should place an appropriate amount of weight on the need to prevent people being drawn into terrorism when they consider all the other factors relevant to how they carry out their usual functions.

‘Extremism’ is defined in the 2011 Prevent strategy as vocal or active opposition to fundamental British values, including democracy, the rule of law, individual liberty and mutual respect and tolerance of different faiths and beliefs. We also include in our definition of extremism calls for the death of members of our armed forces, whether in this country or overseas.

‘Interventions’ are projects intended to divert people who are being drawn into terrorist activity. Interventions can include mentoring, counselling, theological support, encouraging civic engagement, developing support networks (family and peer structures) or providing mainstream services (education, employment, health, finance or housing).

‘Non-violent extremism’ is extremism, as defined above, which is not accompanied by violence.

‘Prevention’ in the context of this document means reducing or eliminating the risk of individuals becoming involved in terrorism. Prevent includes but is not confined to the identification and referral of those at risk of being drawn into terrorism into appropriate interventions. These interventions aim to divert vulnerable people from radicalisation.

‘Radicalisation’ refers to the process by which a person comes to support terrorism and extremist ideologies associated with terrorist groups.

‘Safeguarding’ is the process of protecting vulnerable people, whether from crime, other forms of abuse or (in the context of this document) from being drawn into terrorist-related activity.

The current UK definition of **‘terrorism’** is given in the Terrorism Act 2000 (TACT 2000). In summary this defines terrorism as an action that endangers or causes serious violence to a person/people; causes serious damage to property; or seriously interferes or disrupts an electronic system. The use or threat must be designed to influence the government or to intimidate the public and is made for the purpose of advancing a political, religious or ideological cause.

‘Terrorist-related offences’ are those (such as murder) which are not offences in terrorist legislation, but which are judged to be committed in relation to terrorism.

‘Vulnerability’ describes the condition of being capable of being injured; difficult to defend; open to moral or ideological attack. Within Prevent, the word describes factors and characteristics associated with being susceptible to radicalisation.



Appendix 6

Accessing School Data off Site

USER AGREEMENT

NPW, in partnership with approved 3rd party companies, agree to setup the configuration of your school server to potentially enable sensitive pupil and staff information to be accessed outside of school grounds subject to the terms and conditions stated in this user agreement. By signing this agreement and accessing sensitive data off site you are consenting to be bound by, and are becoming a party to, this agreement. Only employees of Essex Primary School and other approved third parties, authorised by the head teacher, may use sensitive data outside of school grounds. Users are responsible for ensuring that such services are used in a secure way.

School Data can be accessed externally by school staff, who have signed a user agreement, subject to approval by the head teacher and the purchase of the necessary licenses and equipment. NPW should be informed, by the head teacher, of any staff who need to be added or removed as authorised users. Under no circumstances should login credentials, used to access such services, be disclosed and shared amongst colleagues.

Examples of ICT services that potentially allow school data to be accessed off site include but are not limited to:

- LGfL Rav3 Service (remote access to a dedicated school workstation from another remote device)
- SIMS Emerge Service (access to cached MIS data via an approved mobile device, e.g. tablets and phones)
- SIMS Learning Gateway (live web access to SIMS data via the school's SLG web portal)
- Fronter (web access to cached MIS data and other school resources)

In accessing school data off site you are effectively working as in the school environment and therefore subject to the same rules, regulations and guidelines specified within the school's own ICT Security and Usage Policies. As a user accessing school data off site you are responsible for managing the condition of your remote device and should ensure that it is fully protected against any potential configuration changes that could compromise its security.

HARDWARE AND SOFTWARE REQUIREMENTS

By signing this document you agree that your device conforms to the following criteria:

- The operating system should have any available service packs/updates applied
- Where appropriate anti-virus software should be installed and up to date
- If available a suitable software firewall should be enabled
- Where an approved internet browser is required it should be up to date and any security protection options enabled except when this may prevent the service working subject to NPW approval
- When school data is being access from a remote device over a Wi-Fi internet connection the WLAN router should be configured to use the highest available security standard, WPA as a minimum but if supported by your device WPA2 is recommended. Under no circumstances should school data be accessed over an unsecure private or public Wi-Fi connection.

ACCEPTABLE USAGE POLICY

In addition, by signing this document you agree to use school data externally in an appropriate and secure manner that meets the following criteria

- By using school data off site you agree not to disclose any connection or account details that may allow unauthorised access by other users. Usernames, passwords and PIN codes should be kept private and must not be left in written or electronic form in locations where they may be seen by others.
- Services used to access School Data externally should be used only for activity directly related to **Essex Primary School's** work, and should always be in accordance with the school's own ICT Acceptable Usage Policy.
- When accessing school data off site you agree not to compromise confidentiality by opening confidential records (including those held in your MIS and Financial system) in locations where unauthorised persons might see the screen.
- All users agree that they will only print data, originating from your MIS or Financial system, off site when necessary. In such situations, users agree to only print to equipment located in their own home and to ensure there is no unauthorised access to the printed data. All users must be aware that when printing any school data, if such data is viewed by a third party it could be considered a breach of

confidentiality. All users should also take necessary steps to securely store and dispose of such printed material.

- All users agree that they will not keep (or download to the remote device) any sensitive information or other school files. Locally stored files can be accessible to other unauthorised users, are not backed up and may be lost if a device needs to be repaired or replaced. To maintain privacy and prevent potential data loss, it is strongly recommended that all files relating to school duties are saved to an appropriate location on the school network.
- Users authorised to access school data off site agree to use strong passwords, made up of numbers, lower and upper case letters for their network and SIMS accounts. Where PIN codes are used they should be of a varied combination. These passwords or PIN codes should be changed on a regular basis.
- Users must ensure that all devices used to access school data off site are locked and password/PIN code protected when left unattended. Mobile devices should not be left unattended in a public place.
- Users must not try to reconfigure their devices used to access school data in a way that might compromise security.
- Users must not try to save their username, password or PIN code if prompted as part of the login process.
- Users are required to inform the school and NPW if they no longer require off site access to school data (be it via a remote connection or mobile device) and must inform NPW if a configured device is misplaced, rebuilt, replaced or reconfigured by another process.
- All users are required to conform to the Information Security Policy of The London Borough of Newham (<http://newhamintranet/resources/ict/themes/ituserguidesandpolicies.htm>). The information security policy requires that any information seen by a user, such as that held within the school's information management system (SIMS), must be kept private and confidential EXCEPT when it is deemed necessary by law to disclose such information to an appropriate authority. The policy also governs the printing of such information.

I have read, understood and agree to abide by the terms and conditions of the NPW Accessing School Data Off Site User Agreement.

Name:	Signature:
Date:	

Please return to your Data Manager/Head and return a copy to NPW



Department
for Education

Searching, screening and confiscation

**Advice for headteachers, school staff
and governing bodies**

February 2014

Contents

Summary	3
About this departmental advice	3
Expiry or review date	3
Who is this advice for?	3
Key points	3
Screening	5
Searching with consent	6
Searching without consent	7
During the search	10
After the search	11
Frequently Asked Questions	14
Further sources of information	15
Associated resources (external links)	15
Legislative links	15

Summary

About this departmental advice

This advice is intended to explain schools' powers of screening and searching pupils so that school staff have the confidence to use them. In particular it explains the use of the power to search pupils without consent. It also explains the powers schools have to seize and then confiscate items found during a search. It includes statutory guidance which schools must have regard to.

Expiry or review date

This advice will be kept under review and updated as necessary.

Who is this advice for?

This advice is for:

- School leaders and school staff in **all** schools in England.
- For the purposes of this advice references to “maintained school” means a community, foundation or voluntary school, community or foundation special school. It also means Pupil Referral Units and non-maintained special schools.
- For the purpose of this advice references to “Academy” means Academy schools (including mainstream free schools) and AP Academies (including AP Free Schools).
- Where particular provisions do not apply to a particular type of school we make this clear.

Key points

Searching

- School staff can search a pupil for any item if the pupil agrees.¹
- Headteachers and staff authorised by them have a statutory power to search pupils or their possessions, without consent, where they have reasonable grounds for suspecting that the pupil may have a prohibited item. Prohibited items are:
 - knives or weapons
 - alcohol
 - illegal drugs

¹ The ability to give consent may be influenced by the child's age or other factors

- stolen items
- tobacco and cigarette papers
- fireworks
- pornographic images
- any article that the member of staff reasonably suspects has been, or is likely to be, used to commit an offence, or
- to cause personal injury to, or damage to the property of, any person (including the pupil).
- Headteachers and authorised staff can also search for any item banned by the school rules which has been identified in the rules as an item which may be searched for.

Confiscation

- School staff can seize any prohibited item found as a result of a search. They can also seize any item, however found, which they consider harmful or detrimental to school discipline.

Schools' obligations under the European Convention on Human Rights (ECHR)

- Under article 8 of the European Convention on Human Rights pupils have a right to respect for their private life. In the context of these particular powers, this means that pupils have the right to expect a reasonable level of personal privacy.
- The right under Article 8 is not absolute, it can be interfered with but any interference with this right by a school (or any public body) must be justified and proportionate.
- The powers to search in the Education Act 1996 are compatible with Article 8. A school exercising those powers lawfully should have no difficulty in demonstrating that it has also acted in accordance with Article 8. This advice will assist schools in deciding how to exercise the searching powers in a lawful way.

Screening

What the law allows:

- Schools can require pupils to undergo screening by a walk-through or hand-held metal detector (arch or wand) even if they do not suspect them of having a weapon and without the consent of the pupils.
- Schools' statutory power to make rules on pupil behaviour² and their duty as an employer to manage the safety of staff, pupils and visitors³ enables them to impose a requirement that pupils undergo screening.
- Any member of school staff can screen pupils.

Also note:

- If a pupil refuses to be screened, the school may refuse to have the pupil on the premises. Health and safety legislation requires a school to be managed in a way which does not expose pupils or staff to risks to their health and safety and this would include making reasonable rules as a condition of admittance.
- If a pupil fails to comply, and the school does not let the pupil in, the school has not excluded the pupil and the pupil's absence should be treated as unauthorised. The pupil should comply with the rules and attend.
- This type of screening, without physical contact, is not subject to the same conditions as apply to the powers to search without consent.

² Section 89 of the Education and Inspections Act 2006 for all maintained schools, PRUs and NMSS and the Education (Independent School Standards) (England) Regulations 2010 for academy schools and alternative provision academies

³ Section 3 of the Health and Safety at Work etc. Act 1974

Searching with consent

Schools' common law powers to search:

- School staff can search pupils with their consent for any item.

Also note:

- Schools are not required to have formal written consent from the pupil for this sort of search – it is enough for the teacher to ask the pupil to turn out his or her pockets or if the teacher can look in the pupil's bag or locker and for the pupil to agree.
- Schools should make clear in their school behaviour policy and in communications to parents and pupils what items are banned.
- If a member of staff suspects a pupil has a banned item in his/her possession, they can instruct the pupil to turn out his or her pockets or bag and if the pupil refuses, the teacher can apply an appropriate punishment as set out in the school's behaviour policy.
- A pupil refusing to co-operate with such a search raises the same kind of issues as where a pupil refuses to stay in a detention or refuses to stop any other unacceptable behaviour when instructed by a member of staff – in such circumstances, schools can apply an appropriate disciplinary penalty.

Searching without consent

What the law says:

- What can be searched for?
 - Knives or weapons, alcohol, illegal drugs and stolen items; and
 - Tobacco and cigarette papers, fireworks and pornographic images; and
 - Any article that the member of staff reasonably suspects has been, or is likely to be, used to commit an offence, or to cause personal injury to, or damage to property; and
 - Any item banned by the school rules which has been identified in the rules as an item which may be searched for.

1. Can I search?

- Yes, if you are a headteacher or a member of school staff and authorised by the headteacher.

2. Under what circumstances?

- You must be the same sex as the pupil being searched; and there must be a witness (also a staff member) and, if at all possible, they should be the same sex as the pupil being searched.
- There is a limited exception to this rule. You can carry out a search of a pupil of the opposite sex to you and without a witness present, but only where you reasonably believe that there is a risk that serious harm will be caused to a person if you do not conduct the search immediately and where it is not reasonably practicable to summon another member of staff.

3. When can I search?

- If you have reasonable grounds for suspecting that a pupil is in possession of a prohibited item.

Also note:

- The law also says what must be done with prohibited items which are seized following a search.
- The requirement that the searcher is the same sex as the pupil and that a witness is present will continue to apply in nearly all searches. Where it is practicable to summon a staff member of the same sex as the pupil and a witness then the teachers wishing to conduct a search must do so.

4. Authorising members of staff

- Headteachers should decide who to authorise to use these powers. There is no requirement to provide authorisation in writing.
- Staff, other than security staff, can refuse to undertake a search. The law states that headteachers may not require anyone other than a member of the school security staff to undertake a search.
- Staff can be authorised to search for some items but not others; for example, a member of staff could be authorised to search for stolen property, but not for weapons or knives.
- A headteacher can require a member of the school's security staff to undertake a search.
- If a security guard, who is not a member of the school staff, searches a pupil, the person witnessing the search should ideally be a permanent member of the school staff, as they are more likely to know the pupil.

5. Training for school staff

- When designating a member of staff to undertake searches under these powers, the headteacher should consider whether the member of staff requires any additional training to enable them to carry out their responsibilities.

6. Establishing grounds for a search

- Teachers can only undertake a search without consent if they have reasonable grounds for suspecting that a pupil may have in his or her possession a prohibited item. The teacher must decide in each particular case what constitutes reasonable grounds for suspicion. For example, they may have heard other pupils talking about the item or they might notice a pupil behaving in a way that causes them to be suspicious.
- In the exceptional circumstances when it is necessary to conduct a search of a pupil of the opposite sex or in the absence of a witness, the member of staff conducting the search should bear in mind that a pupil's expectation of privacy increases as they get older.
- The powers allow school staff to search regardless of whether the pupil is found after the search to have that item. This includes circumstances where staff suspect a pupil of having items such as illegal drugs or stolen property which are later found not to be illegal or stolen.
- School staff can view CCTV footage in order to make a decision as to whether to conduct a search for an item .

7. Searches for items banned by the school rules

- An item banned by the school rules may only be searched for under these powers if it has been identified in the school rules as an item that can be searched for.
- The school rules must be determined and publicised by the headteacher in accordance with section 89 of the Education and Inspections Act 2006 in maintained schools. In the case of academy schools and alternative provision academies, the

school rules must be determined in accordance with the School Behaviour (Determination and Publicising of Measures in Academies) Regulations 2012. Separate advice on school rules is available in 'Behaviour and Discipline – advice for headteachers and school staff' via the link under Associated Resources.

- Under section 89 and the School Behaviour (Determination and Publicising of Measures in Academies) Regulations 2012 the headteacher must publicise the school behaviour policy, in writing, to staff, parents and pupils at least once a year.

8. Location of a search

- Searches without consent can only be carried out on the school premises or, if elsewhere, where the member of staff has lawful control or charge of the pupil, for example on school trips in England or in training settings.
- The powers only apply in England.

During the search

9. Extent of the search – clothes, possessions, desks and lockers

What the law says:

- The person conducting the search may not require the pupil to remove any clothing other than outer clothing.
- ‘Outer clothing’ means clothing that is not worn next to the skin or immediately over a garment that is being worn as underwear but ‘outer clothing’ includes hats; shoes; boots; gloves and scarves.
- ‘Possessions’ means any goods over which the pupil has or appears to have control – this includes desks, lockers and bags.
- A pupil’s possessions can only be searched in the presence of the pupil and another member of staff, except where there is a risk that serious harm will be caused to a person if the search is not conducted immediately and where it is not reasonably practicable to summon another member of staff.

Also note:

- The power to search without consent enables a personal search, involving removal of outer clothing and searching of pockets; but not an intimate search going further than that, which only a person with more extensive powers (e.g. a police officer) can do.

10. Lockers and desks

- Under common law powers, schools are able to search lockers and desks for any item provided the pupil agrees. Schools can also make it a condition of having a locker or desk that the pupil consents to have these searched for any item whether or not the pupil is present.
- If a pupil does not consent to a search (or withdraws consent having signed a consent form) then it is possible to conduct a search without consent but only for the “prohibited items” listed above.

11. Use of force

- Members of staff can use such force as is reasonable given the circumstances when conducting a search for knives or weapons, alcohol, illegal drugs, stolen items, tobacco and cigarette papers, fireworks, pornographic images or articles that have been or could be used to commit an offence or cause harm. Such force cannot be used to search for items banned under the school rules.
- Separate advice is available on teachers’ power to use force – see Associated Resources section below for a link to this document

After the search

12. The power to seize and confiscate items – general

What the law allows:

- Schools' general power to discipline, as set out in Section 91 of the Education and Inspections Act 2006, enables a member of staff to confiscate, retain or dispose of a pupil's property as a disciplinary penalty, where reasonable to do so.

Also note:

- The member of staff can use their discretion to confiscate, retain and/or destroy any item found as a result of a 'with consent' search so long as it is reasonable in the circumstances. Where any article is thought to be a weapon it must be passed to the police.
- Staff have a defence to any complaint or other action brought against them. The law protects members of staff from liability in any proceedings brought against them for any loss of, or damage to, any item they have confiscated, provided they acted lawfully.

13. Items found as a result of a 'without consent' search

What the law says:

- A person carrying out a search can seize anything they have reasonable grounds for suspecting is a prohibited item or is evidence in relation to an offence.
- Where a person conducting a search finds alcohol, they may retain or dispose of it. This means that schools can dispose of **alcohol** as they think appropriate but this should not include returning it to the pupil.
- Where they find **controlled drugs**, these must be delivered to the police as soon as possible but may be disposed of if the person thinks there is a good reason to do so.
- Where they find **other substances** which are not believed to be controlled drugs these can be confiscated where a teacher believes them to be harmful or detrimental to good order and discipline. This would include, for example, so called 'legal highs'. Where staff suspect a substance may be controlled they should treat them as controlled drugs as outlined above.
- Where they find **stolen items**, these must be delivered to the police as soon as reasonably practicable – but may be returned to the owner (or may be retained or disposed of if returning them to their owner is not practicable) if the person thinks that there is a good reason to do so.
- Where a member of staff finds **tobacco or cigarette papers** they may retain or dispose of them. As with alcohol, this means that schools can dispose of tobacco or cigarette papers as they think appropriate but this should not include returning them to the pupil.

- **Fireworks** found as a result of a search may be retained or disposed of but should not be returned to the pupil.
- If a member of staff finds a **pornographic image**, they may dispose of the image unless its possession constitutes a specified offence (i.e. it is extreme or child pornography) in which case it must be delivered to the police as soon as reasonably practicable. Images found on a mobile phone or other electronic device can be deleted unless it is necessary to pass them to the police.
- Where an **article that has been (or could be) used to commit an offence or to cause personal injury or damage to property** is found it may be delivered to the police or returned to the owner. It may also be retained or disposed of.
- Where a member of staff finds **an item which is banned under the school rules** they should take into account all relevant circumstances and use their professional judgement to decide whether to return it to its owner, retain it or dispose of it.
- Any **weapons or items which are evidence of an offence** must be passed to the police as soon as possible.

14. Statutory guidance on the disposal of controlled drugs and stolen items

- It is up to teachers to decide whether there is a good reason not to deliver stolen items or controlled drugs to the police. In determining what is a “good reason” for not delivering controlled drugs or stolen items to the police the member of staff must have regard to the following guidance issued by the Secretary of State :
- **In determining what is a ‘good reason’ for not delivering controlled drugs or stolen items to the police, the member of staff should take into account all relevant circumstances and use their professional judgement to determine whether they can safely dispose of a seized article.**
- Where staff are unsure as to the legal status of a substance and have reason to believe it may be a controlled drug they should treat it as such.
- With regard to stolen items, it would not be reasonable or desirable to involve the police in dealing with low value items such as pencil cases. However, school staff may judge it appropriate to contact the police if the items are valuable (iPods/laptops) or illegal (alcohol/fireworks).

15. Statutory guidance for dealing with electronic devices

- Where the person conducting the search finds an electronic device they may examine any data or files on the device if they think there is a good reason to do so. Following an examination, if the person has decided to return the device to the owner, or to retain or dispose of it, they may erase any data or files, if they think there is a good reason to do so.
- The member of staff must have regard to the following guidance issued by the Secretary of State when determining what is a “good reason” for examining or erasing the contents of an electronic device:
- In determining a ‘good reason’ to examine or erase the data or files the staff member must reasonably suspect that the data or file on the device in question has been, or

could be, used to cause harm, to disrupt teaching or break the school rules.

- If inappropriate material is found on the device it is up to the teacher to decide whether they should delete that material, retain it as evidence (of a criminal offence or a breach of school discipline) or whether the material is of such seriousness that it requires the involvement of the police.

Also note:

- Teachers should also take account of any additional guidance and procedures on the retention and disposal of items that have been put in place by the school.

16. Telling parents and dealing with complaints

- Schools are not required to inform parents before a search takes place or to seek their consent to search their child.
- There is no legal requirement to make or keep a record of a search.
- Schools should inform the individual pupil's parents or guardians where alcohol, illegal drugs or potentially harmful substances are found, though there is no legal requirement to do so.
- Complaints about screening or searching should be dealt with through the normal school complaints procedure.

Frequently Asked Questions

Q: I'm a teacher; can I refuse to search a pupil without their consent?

A: Yes. A headteacher cannot require a member of staff to conduct a search. In order to conduct a search without consent, a member of staff must be authorised to do so. Staff can choose whether they want to be authorised, or not.

Q: Is there a risk that I could face legal challenge if I search a pupil without consent?

A: Headteachers and authorised school staff have a specific statutory power to search pupils without consent for specific items – knives/weapons, alcohol, illegal drugs and stolen items. As long as the member of staff acts within the limits of this specific power they will have a robust defence against a legal challenge.

Further sources of information

Associated resources (external links)

- [Use of Reasonable Force – advice for headteachers, staff and governing bodies Behaviour and Discipline in Schools](#)
- [Behaviour and Discipline in Schools – advice for head teachers and school staff](#)
- [Information Commissioner for advice on the Data Protection Act](#)

Legislative links

- [The Education Act 1996](#)
- [Education and Inspections Act 2006](#)
- [Education \(Independent School Standards\) \(England\) Regulations 2010](#)
- [The Schools \(Specification and Disposal of Articles\) Regulations 2012](#)
- [School Behaviour \(Determination and Publicising of Measures in Academies\) Regulations 2012](#)
- [Health and Safety at Work etc Act 1974](#)



Department
for Education

© Crown copyright 2015

This publication (not including logos) is licensed under the terms of the Open Government Licence v3.0 except where otherwise stated. Where we have identified any third party copyright information you will need to obtain permission from the copyright holders concerned.

To view this licence:

visit www.nationalarchives.gov.uk/doc/open-government-licence/version/3

email psi@nationalarchives.gsi.gov.uk

write to Information Policy Team, The National Archives, Kew, London, TW9 4DU

About this publication:

enquiries www.education.gov.uk/contactus

download www.gov.uk/government/publications

Reference: DFE-00034-2014



Follow us on Twitter:
[@educationgovuk](https://twitter.com/educationgovuk)



Like us on Facebook:
facebook.com/educationgovuk