ESSEX PRIMARY SCHOOL

Online Safety

Policy

Reviewed September 2021

Next Review due September 2022

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

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: How will infringements be handled?

1. Introduction and Overview

At Essex Primary we believe that Computing/ICT is central to all aspects of learning; for adults and children in both the school and the wider community. Provision should reflect the rapid developments in technology.

Computing/ICT in the 21st Century is an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, we need to build in the use of these technologies in order to equip our young people with the skills to access lifelong learning and employment.

All children, whatever their needs, will have access to a range of up to date technologies in school. ICT is a life skill and should not be taught in isolation.

Information and Communications Technology covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies children are using both inside and outside of the classroom include:

- Websites
- Learning Platforms and Virtual Learning Environments
- Email and Instant Messaging
- Chat Rooms and Social Networking
- Blogs
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices with web functionality

All users need to be aware of the range of risks associated with the use of these Internet technologies.

At Essex Primary School, we understand the responsibility to educate our pupils on online-safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

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 pupils and staff.
- Assist school staff working with pupils 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 pupils.

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
Head Teacher	• Must be adequately trained in off-line and online safeguarding, inline 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 andharmsprovision • 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
Online Safety Coordinator/ Designated Child Protection Lead (This may be the same person)	• 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
	• 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)	• 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 coordinator
Computing Curriculum Leader	• To oversee the delivery of the online safety element of the Computing curriculum • Keep up-to-date with current research, legislation and trends regarding online safety • Coordinate participation in local and national events to promote positive online behaviour, e.g. Safer Internet Day • Ensure that online safety is promoted to parents and carers and the wider community through a variety of channels and approaches

Network Manager/ Technician (SBT)	• To report online safety related issues that come to their attention, to the Online Safety Coordinator • To ensure school password policy is strictly adhered to • To ensure systems are in place for misuse detection and malicious attack (e.g. keeping virus protection up to date) • To ensure access controls/encryption exist to protect personal and sensitive information held on school-owned devices • To ensure the school's policy on web filtering is applied and updated on a regular basis • Must 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 • To ensure that the use of school technology and online platforms are regularly monitored and that any misuse/attempted misuse is reported to the online safety coordinator/Executive Head Teacher • To ensure appropriate backup procedures and disaster recovery plans are in place • To keep up-to-date documentation of the school's online security and technical procedures
LGfL Nominated contact(s)	• To ensure all LGfL services are managed on behalf of the school following data handling procedures as relevant
Teachers	• 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

All staff	• 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 • Maintain a professional level of conduct in their personal use of technology, both on and off site. **Exit strategy** • At the end of the period of employment/volunteering to return any equipment or devices loaned by the school. This will include leaving Laptops, 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.
Pupils	• Read, understand, sign and adhere to the 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 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 • To contribute to any 'pupil voice' / surveys that gathers information of their online experiences • Respect the feelings and rights of others both on and offline. • Take responsibility for keeping themselves and others safe online.

Parents/ Carers	• To read, understand and promote the school's Pupil Acceptable Use Agreement with their child/ren • To discuss online safety issues with their children, supporting the school in their online safety approaches, and reinforcing appropriate safe online behaviours at home • Role model safe and appropriate uses of technology and social media • Identify changes in behaviour that could indicate that their child is at risk of harm online. • Seeking help and support from the school, or other appropriate agencies, if they or their child encounters online problems or concerns • Use school systems, such as learning platforms, and other network resources, safely and appropriately • Take responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies
External groups including Parent groups	• 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 and on Google Drive
- 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 and harms.
- Staff and pupils are given information about infringements in use and possible sanctions – see appendix 4.
- Online Safety Coordinator (Designated Safeguarding Lead) 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 Executive Head Teacher, unless the concern is about the Executive Head Teacher 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. Child Protection and Safeguarding 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.
- 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:

- provides 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

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 pupils 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 and child friendly search terms 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, Newham Partnership Working, 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
- Uses secure, 'Cloud' storage (G- suite – Google) 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.
- Ensures 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.

Passwords

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.
- Ensures all staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password(s) private.
- Requires staff to use STRONG passwords.
- Requires staff to change their passwords into the MIS, LGfL USO admin site, every 90 days/twice a year.
- Requires 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.
- Uses 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.
- 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:

- Use LGfL pupil email system which is intentionally 'anonymised' for pupil protection.
- May only use school/setting provided email accounts for educational purposes.
- Are taught about the online safety and 'netiquette' of using e-mail both in school and at home.

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.
- Will be encouraged to develop an appropriate work life balance when responding to email.

School website

- The Head Teacher, 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 (G-suite / Google)

- Uploading of information on the school's online learning space is shared between different staff members according to their responsibilities e.g. all class teachers upload information in their class/Year group 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/Google' 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.
- They should not be online friends with any pupil/student. Any exceptions must be approved by the Executive Head Teacher.
- 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 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.
- Are required to sign and follow our [age appropriate] pupil Acceptable Use Agreement - Appendix 2.

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 Executive Head Teacher is the Senior Information Risk Officer (SIRO).
- Staff are clear who are the key contact(s) for key school information and the Information Asset Owners. 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 Executive Head Teacher. Such authorised use is to be recorded. All mobile device use is to be open to monitoring scrutiny and the Executive Head Teacher 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 Executive 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 brought 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 Executive Head Teacher / 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 pupils 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 Executive Head Teacher / 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/carer 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 (AUP) 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 use.
- The school blocks/filters 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.

A London Grid for Learning / TRUSTnet brand

	Name of School	**Essex Primary School**
	AUP review Date	**September 2021**
	Date of next Review	**September 2022**
	Who reviewed this AUP?	**Amber Ilyas / NPW**

Acceptable Use Agreement: Staff, Volunteers, Governors & Contractors

Essex Primary School regularly reviews and updates all AUP documents to ensure that they are consistent with the school Online Safety Policy.

These rules will help to keep everyone safe and to be fair to others. Please note that school systems and users are protected and monitored by security and filtering services to provide safe access to digital technologies. Your behaviour online when in school and on all school devices whether in school or otherwise may therefore be subject to monitoring.

- 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 and change my passwords regularly. 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 / intranet / network / social networks / mobile apps / or any other system I have access to via the school or school umbrella.
- 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 Staffmail
- I will only use the approved method/s of communicating with pupils or parents/carers: LGFL StaffMail Learning Platform (Google Classroom), online cloud storage service (Google Drive), and only communicate with them in a professional manner and on appropriate school business.
- I will not support or promote extremist organisations, messages or individuals.
- I will not give a voice or opportunity to extremist visitors with extremist views.
- 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 Child Protection Officer and 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 use USBs on any school equipment, Google drive will be used as the main storage device for all teaching and learning materials.
- 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 or on any personal devices.
- I will follow the school's policy (see Staff handbook) on use of mobile phones / devices at school and will not use in the classrooms / only use in staff areas.
- 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 only take or publish images of staff and students with their permission and in accordance with the school's policy on the use of digital / video images. Images published on the school website, online learning environment etc. will not identify students by name, or other personal information.
- I will use the school's Learning Platform or online cloud storage service 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 Google Drive/ 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 am aware that under the provisions of the GDPR (General Data Protection Regulation), my school and I have extended responsibilities regarding the creation, use, storage and deletion of data, and I will not store any pupil data that is not in line with the school's data policy and adequately protected. The school's data protection officer must be aware of all data storage.
- I will alert Essex Primary School DSL/CP 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 the relevant Senior Member of Staff / Designated Safeguarding Lead.
- I understand that all internet and network traffic / usage can be logged and this information can be made available to the Head / Designated 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 understand that I have a responsibility to uphold the standing of the teaching profession and of the school, and that my digital behaviour can influence this.
- Staff that have a teaching role only: I will embed the school's online 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' e-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 / Safeguarding Policies.

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

Signature ..... Date .....

Full Name ..... (printed)

Job title / Role .....

Authorised Signature (Executive / Associate Head Teacher)

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

Signature ..... Date .....

Full Name ..... (printed)

LGfL DigiSafe

A London Grid for Learning / TRUSTnet brand

Key Stage 1: Acceptable Use Agreement

This is how I keep **SAFE online**:	✓
1. I only use the devices I'm **ALLOWED** to	
2. I **CHECK** before I use new sites, games or apps	
3. I **ASK** for help if I'm stuck	
4. I **THINK** before I click	
5. I **KNOW** people online aren't always who they say	
6. I don't keep ~~**SECRETS**~~ just because someone asks me to	
7. I don't change **CLOTHES** in front of a camera	
8. I am **RESPONSIBLE** so never share private information	
9. I am **KIND** and polite to everyone	
10. I **TELL** a trusted adult if I'm worried, scared or just not sure	

My trusted adults are:

_____ **at school**

_____ **at home**

_____ **(Others)**

My name is _____ **Date:** _____ **Class:** _____

A London Grid for Learning / TRUSTnet brand

KS2 Pupil Online Acceptable Use Agreement

This agreement will help keep me safe and help me to be fair to others

- ***I am an online digital learner*** – I use the school's internet and devices for schoolwork, homework and other activities to learn and have fun. I only use sites, games and apps that my trusted adults say I can.
- ***I am a secure online learner*** – I keep my passwords to myself and reset them if anyone finds them out.
- ***I am careful online*** – I think before I click on links and only download when I know it is safe or has been agreed by trusted adults. I understand that some people might not be who they say they are, so I should be very careful when someone wants to be my friend.
- ***I am private online*** – I only give out private information if a trusted adult says it's okay. This might be my home address, phone number or other personal information that could be used to identify me or my family and friends.
- ***I keep my body to myself online*** – I never change what I wear in front of a camera and remember that my body is mine and mine only, and I don't send any photos without checking with a trusted adult.
- ***I say no online if I need to*** – if I get asked something that makes me worried or upset or just confused, I say no, stop chatting and tell a trusted adult.
- ***I am a rule-follower online*** – I know that some websites and social networks have age restrictions and I respect this; I only visit sites, games and apps that my trusted adults have agreed to.
- ***I am considerate online*** – I do not join in with bullying or sharing inappropriate material.
- ***I am respectful online*** – I do not post, make or share unkind, hurtful or rude messages/comments and tell my trusted adults if I see these.
- ***I am part of a community*** – I do not make fun of anyone or exclude them because they are different to me. If I see anyone doing this, I tell a trusted adult.
- ***I am responsible online*** – I keep others safe by talking to my trusted adults if a friend or person I know is being bullied or harassed or is worried or upset by things they read, watch or hear.

- ***I don't do public live streams on my own*** – and only go on a video chat if my trusted adult knows I am doing it and with whom.
- ***I communicate and collaborate online*** – with people I know and have met in real life or that a trusted adult knows about.
- ***I am SMART online*** – I understand that unless I have met people in real life, I can't be sure who someone is online, so if I want to meet someone for the first time, I must always ask a trusted adult for advice.
- ***I am a creative digital learner online*** – I don't just spend time online to look at things from other people; I get creative to learn and make things! I only edit or delete my own digital work and only use other people's with their permission or where it is copyright free or has a Creative Commons licence.
- ***I am a researcher online*** – I use safer search tools approved by my trusted adults. I understand that not everything online can be believed, but I know how to check things and know to 'double check' information I find online.

I have read and understood this agreement. I know who my trusted adults are and agree to the above.

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 include 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.

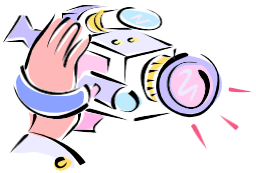
I understand that the school takes any inappropriate behaviour seriously and will respond to observed or reported inappropriate or unsafe behaviour.

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):_____ **Class:** _____

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 comply with 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.

Staff 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 libelous 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/

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:**
• 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	**Refer to class teacher / tutor** Escalate to: Senior Manager / Online-Safety Coordinator Use Behaviour Policy
Category B infringements	**Possible Sanctions:**
• 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 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	**Refer to Class teacher/ Head of Year / Phase Leader / Online-Safety Coordinator** Escalate to: removal of Internet access rights for a period / removal of phone until end of day / contact with parent

STUDENT	
Category C infringements	**Possible Sanctions:**
• 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	**Refer to Class teacher / Year Group Lead / Phase Leader /Online-Safety Coordinator / Head teacher / removal of Internet and/or Learning Platform access rights for a period** Escalate to: contact with parents / removal of equipment **Other safeguarding actions if inappropriate web material is accessed:** Ensure appropriate technical support filters the site
Category D infringements	**Possible Sanctions:**
• 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	**Refer to Executive Head Teacher / Contact with parents** **Other possible safeguarding actions:** • 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:**
• 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.	**Referred to line manager / Executive Head Teacher** Escalate to: *Warning given (Management Action Procedure)*
Category B infringements (Gross Misconduct)	**Possible Sanctions:**
• 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	**Referred to Executive Head Teacher / Governors;** **Other safeguarding actions:** ▪ 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. *Escalate to:* *report to LA /LSCB, Personnel, Human resource.* Report to Police / CEOP where child abuse or illegal activity is suspected. Management Action procedures / Disciplinary Action

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