Online Safety Policy

June 2017

Edinburgh Primary School

Edinburgh Primary School – Online Safety Policy 2017/ 2018

97 Queens Road, Walthamstow, London, E17 8QR

Edinburgh Primary School

Online Safety Policy – June 2017 (to be reviewed June 2018)

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

Contents

Asset Disposal. 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: Protocol for responding to online - safety incidents http://www.lgfl.net/esafety/Pages/policies-acceptable-use.aspx - handling infringements

A4: What to do if? – Staff guidance on different scenarios

A5: Data security: Use of IT systems and Data transfer

Search and Confiscation guidance from DfE https://www.gov.uk/government/publications/searching-screening-and-confiscation (not attached to document)

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 Edinburgh 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 [in line with the school's anti-bullying, behaviour and safeguarding policies].
- 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 primary 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)
- The sending of inappropriate text, image and movie messages
- Copyright (little care or consideration for intellectual property and ownership)

Scope

This policy applies to all members of Edinburgh Primary School’s community (including staff, governors, students/pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of any of the school’s ICT systems.

Roles and responsibilities

Role	Key Responsibilities
Headteacher / Safeguarding lead	• 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 (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 or exposed to other inappropriate material • To receive regular monitoring reports from the Online Safety leader • 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 updated, as necessary, on the nature and effectiveness of the school's arrangements for online safety • To ensure school website includes relevant information.
Computing Leader/ Safeguarding 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, in liaison with the school's PSHE and

Role	Key Responsibilities
	Computing curriculum • Liaise with school technical staff where appropriate • To communicate, where appropriate, with SLT and the designated online safety/ safeguarding Governor 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 as needed • Is regularly updated in online safety issues and legislation, and be aware of the potential for serious child protection concerns.
Governors/Safeguarding governor	• 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 Safe Guarding Governor will include: regular reviews ofOnline Safety with the Safe Guard Lead.
Computing Curriculum Leader	• To oversee the delivery of the online safety element of the Computing curriculum
PSHE Curriculum Leader	• To incorporate online safety element as part of the school's anti-bullying curriculum
Network Manager (Joskos)/technician	• To report online safety related issues that come to their attention, to the Computing Leaders • To manage the school's computer systems, ensuring - 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)

Role	Key Responsibilities
	- 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, including keeping appropriate logs • 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 [Google Apps for Education and school website] are regularly monitored and that any misuse/attempted misuse is reported to the online safety leader / Headteacher • 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
Data and Information Managers (IAOs) / School Business Manager	• 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
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 in 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, volunteers and contractors.	• 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.

Role	Key Responsibilities
	• To report any suspected misuse or problem to the online safety leaders/ headteacher • 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
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
Parents/carers	• 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 Acceptable Use Agreement which includes the pupils' use of the Internet and the school's use of photographic and video images – consent is sought during pupil admission meetings
External groups including Parent groups	• 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. Information for pupils will be displayed in standardised poster form in all classrooms. The policy and will be made available on the school's ICT network for all staff.
- 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:

- The school will take all reasonable precautions to ensure Online Safety.
- Staff and pupils are given information about infringements in use and possible sanctions.
- The Computing leaders act as first point of contact for any incident.
- Any suspected online risk or infringement is reported to the Computing Leaders/ school technician/ as soon as possible.
- Any concern about staff misuse is always referred directly to the Headteacher, unless the concern is about the Headteacher in which case the compliant is referred to the Chair of Governors and the LADO (Local Authority's Designated Officer).

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 as part of the Computing curriculum and is referenced in the PSHE curriculum. This covers a range of skills and behaviours appropriate to their age and experience;
- plans online use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas;
- will remind pupils about their responsibilities through the pupil Acceptable Use Agreement(s);
- 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;
- 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;
- ensure pupils only use school-approved systems and publish within appropriately secure / age-appropriate environments.

Staff 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 advice for parents which includes online safety;
- 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;
- support is actively sought from other agencies as needed (i.e. the local authority, LGfL, UK Safer Internet Centre helpline, CEOP, Prevent Officer, Police, 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, linking with the behaviour lead (DHT) as required;
- 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 as required.

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.ensures network health through use of Sophos anti-virus software (from LGfL);
- Uses DfE, LA or LGfL approved systems such as (but not limited to) DfE S2S, 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 for school email and online teaching & learning resources, and individual log-ins provided by the school's ICT support provider (currently Joskos). In the Early Years and Key Stage 1, class log-ins are used and are transitioned to individual log-ins in preparation for Key Stage 2.
- Uses guest accounts for external or short term visitors for temporary and limited 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 (currently LGfL Gridstore)
- 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 acceptable use 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
- All Key Stage 2 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 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 (in exceptional circumstances) by the school, is used primarily to support their professional responsibilities.
- Maintains equipment to ensure Health and Safety is followed;
- Ensures that access to the school's network resources from remote locations by staff is audited and restricted and access is only through school/LA approved systems:
- 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 or only sent within the approved secure system in our LA or through USO secure file exchange (USO FX);
- 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 and are responsible for changing/ seeking support to change if they feel the security of the credentials have been breached.
- We require staff using critical systems to use two factor authentication. This primarily applies to school nominated contacts for LGFL – all of whom are provided with an OTP tag.

E-mail

This school

- Provides staff with an email account for their professional use, London Staffmail and makes clear personal email should be through a separate account;
- We may use anonymous or group e-mail addresses, for example school@edinburgh.waltham.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. We also use Google Apps for Education which is an internal online application whereby pupils can only contact members of the school community – it is impossible for pupils to be contacted by external internet users.
- Pupils are taught about the online safety and 'netiquette' of using e-mail both in school and at home.

Staff:

- Staff can only use LGfL email systems on the school system for school business. Google Apps for Education accounts are used to support the online learning of pupils e.g. to receive homework
- Access in school to external personal email accounts may be blocked if it is deemed the provider is unsuitable, or the goodwill of use is being abused
- Never use email to transfer sensitive staff or pupil personal data. 'Protect-level' data should never be transferred by email.

School website

- The Headteacher 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 year group areas;
- Photographs and videos uploaded to the school's online environment will not name individual pupils;
- 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 (Google Apps for Education) for such communications, where deemed necessary to enhance teaching and learning.
- Edinburgh Primary School does not currently have an external social media presence e.g. a Facebook page/ twitter account. Should this be created, a protocol of use would be published.

School staff will ensure that in private use:

- No reference should be made in social media to pupils, parents/carers or school staff;
- School staff should not be online friends with any pupil. 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 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.
- Pupils are required to sign and follow our age appropriate pupil Acceptable Use Agreement.

Parents:

- Parents are reminded about social networking risks and protocols through our parental Acceptable Use Agreement and additional communications materials when required. Parents are reminded through the school website and newsletters.
- Are reminded that they need to ask permission before uploading photographs, videos or any other information about other people within the school community.

Sexting

'Sexting' is one of a number of 'risk-taking' behaviours associated with the use of digital devices, social media or the internet. It is accepted that young people experiment and challenge boundaries and therefore the risks associated with 'online' activity can never be completely eliminated.

However, Edinburgh Primary School takes a pro-active approach to help students and staff to understand, assess, manage and avoid the risks associated with 'online activity'. The school recognises its duty of care to its young people and staff who do find themselves involved in such activity as well as its responsibility to report such behaviours where legal or safeguarding boundaries are crossed.

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. This is the headteacher and business manager.
- 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 of workstations during idle periods.
- 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.

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, pupils & 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.
- Mobile devices brought in to school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally-owned mobile devices.
- Year 6 pupils are permitted to bring mobile phones to school so that they can be contacted by their parents to/from school. Student personal mobile devices, which are brought into school, must be turned off (not placed on silent) and stored out of sight on arrival at school. They must remain turned off and out of sight until the end of the day. A letter of permission must be sought from parents. Children in all other year groups are not permitted to bring a mobile phone to school, unless exceptional circumstances lead to the headteacher permitting the use on an individual basis.
- Personal mobile devices are not permitted to be used by staff during pupil contact time and when pupils are in view. Staff members may use their phones during school break times – but not when on duty.
- No images or videos should be taken on mobile devices without the prior consent of the person or people concerned. This includes school mobile devices i.e. iPads.
- 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. Staff mobiles devices may be searched should there be significant concern. Safeguarding procedures would apply.
- 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.
- 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.

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 network manager.

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.

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;
- If an image / media file is used as part of any school marketing/promotion e.g. the school website, parents and carers may request the image to be removed. The school will communicate with parents on this issue. Where external use of pupil images are to be used e.g. the local newspaper, multi-school project, Edinburgh will seek additional permission from parents and carers;
- 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;
- The school blocks/filter access to social networking sites unless there is a specific approved educational purpose;
- 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.

Appendices

These appendices reflect practice as of September 2017

Edinburgh Primary School

ICT Acceptable Use Agreement – Staff, Volunteers & Governors

Review: Summer 2017 Date of next review: Summer 2018

This agreement covers the use of all digital technologies in school: i.e. email, Internet, network resources, learning platform, software, communication tools, equipment and systems. Before using the school's ICT network, you must read and agree to the statements below:

- 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 system I have access to*.
- I will not engage in any online activity that may compromise my professional responsibilities.
- I will only use the approved email system for any school business.
  This is currently LGFL Staff Mail.
- I will only use the approved *email system (London Mail/ TrustMail)*, *Learning Platform (Google Apps for Education) and school approved communication systems (including the school blogs)* 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 *appropriate school named contact*.
- 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 ICT 'defence' systems*. I am aware that the school provides free anti-virus for use at home – Sophos- as part of LGFL.
- 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 on use of mobile phones and *only use when out of pupil view.*
- 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 *staff-only drive within school* (T drive). Photos will be stored in the 'photos' folder.

- I will use the school's Learning Platform 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 and that I will notify the school of any "significant personal use" as defined by HM Revenue & Customs.
- 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 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 *the online safety/ safeguarding lead* 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 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 / Safeguarding lead* on their request.
- I understand that Internet encrypted content 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 curriculum into my teaching.

Acceptable Use Agreement/Policy Declaration

I , (name) ……………………………………………………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 e-safety policies.

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

Role ……………………………………………………………………………………………

Signature: ……………………………………………… **Date …………………………………..**

Edinburgh Primary School

Pupil Acceptable Use Policy Agreement – Key Stage 1

We endeavour to teach our children to be responsible users of ICT and provide them with the guidance necessary to keep them safe when using online technologies. The school will try to ensure that our children will have good access to ICT to enhance their learning, but in return will expect the children to agree to be responsible users. In Key Stage 1, the following will be read to pupils for them to understand:

This is how we stay safe at Key Stage 1 when we use computers:

- I will ask a teacher / an adult if I want to use the computer.
- I will only use applications that the teacher /an adult has told or allowed me to use.
- I will take care of the computers and other ICT equipment.
- I will ask for help from the teacher / an adult if I am not sure what to do or if I think I have done something wrong.
- I will tell the teacher / an adult if I see something that upsets me on the screen.
- I know not to talk to strangers online.
- I will keep my personal information and passwords safe.
- I will always be nice if I post or put up messages online.
- I know that if I break the rules I might not be allowed to use the school's ICT equipment until I am safe to do so.

I understand the Pupil Acceptable Use Agreement.

Name ……………………………………………,,,,,,,,, Class …………………………………..

Edinburgh Primary School

Pupil Acceptable Use Policy Agreement – Key Stage 2

This acceptable use policy should be understood and signed upon joining Key Stage 2 and reviewed annually.

At Edinburgh Primary, we teach our children to be responsible users of ICT and provide them with the guidance necessary to keep them safe when using online technologies. The school will aim to ensure that our children will have good access to ICT to enhance their learning, but in return will expect the children to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use the school's ICT resources in a responsible manner, to make sure that I keep myself and others safe whilst working online.

Personal Safety

- I will keep my passwords safe and will not use other people's passwords
- I will be aware of "stranger danger", when working online.
- I will not share personal information about myself or others when on-line.
- I will not upload any images of myself or of others without permission
- I will not arrange to meet up with people that I have communicated with online.
- I will immediately report any inappropriate material, messages I receive or anything that makes me feel uncomfortable when I see it online.
- I will learn how to use the 'thinkuknow' web site to keep myself safe.
- I will report any bad behaviour by telling a responsible adult and will learn about using the CEOP Report button.
- I know that the school can look at my use of ICT and what I use online ICT

Property and Equipment

- I will respect all computing/ ICT equipment and will report any damage or faults.
- I will respect others' work and will not access, copy, move or remove files.
- I will not use mobile phones/USB devices in school without permission.
- I will not use any programs or software without permission.
- I will not use or open email, unless I know and trust the person or organisation.
- I will not install programs or alter any computer settings, including web browser homepages.

- I will only use approved and moderated chatrooms or social networking sites with permission from a responsible adult

Cyber Bullying

- I will be polite when I communicate with others
- I know not to do online what I wouldn't do offline like in the playground
- I will not use inappropriate language or make unkind comments
- I appreciate others may have different opinions
- I will not upload or spread images of anyone

The Internet

- I understand that I need permission to be on the Internet.
- I will not fill in any online forms without adult permission
- I will not use any sites I've not had permission to use, this includes social media sites that I'm not old enough to use
- I will learn about copyright laws and make sure I acknowledge resources
- I will not upload or download images, music or videos without permission
- I will check that the information that I access on the internet is accurate, as I understand that the internet may not be truthful and may mislead me.

Outside of the School Community

- I understand that this agreement is for in and outside the school
- I know there will be consequences if I am involved in incidents of inappropriate behaviour covered in this agreement

I understand the Pupil Acceptable Use Agreement for using technology, internet, email and online tools safely.

Name ……………………………………………………………………………………

Date ………………………………… Signature ……………………………………

Appendix 3: How will infringements be handled at Edinburgh Primary School?

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

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

Pupil	
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** Escalate to: senior manager / Online-Safety lead/ behaviour lead
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 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	**Refer to Class teacher/ Year group / phase leader tutor / Online-Safety lead/ behaviour lead** Escalate to: removal of Internet access rights for a period / removal of phone until end of day / contact with parent]

Pupil	
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 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 / phase leader tutor / Online-Safety lead/ behaviour lead/ Headteacher** **/ 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 inappropriate emails or 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 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. during contact time • 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 / Head teacher** Escalate to: *Warning given*
Category B infringements (Gross Misconduct)	**Possible Sanctions:**
• Serious misuse of, or deliberate damage to, any school / LA 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 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 /, Personnel, Human resource.* Report to Police / CEOP where child abuse or illegal activity is suspected.

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).

Edinburgh Primary School – Online Safety Staff Guidance:

What would you do if…?

Please familiarise yourself with the scenarios below which offer guidance on what to do should an e-safety concern arise. If you have any questions regarding this, please speak to the Online Safety Leader.

- **An inappropriate website is accessed unintentionally in school by a teacher or child.**

1. Play the situation down; don't make it into a drama. Take it as a learning/teaching point.

2. Report to the head teacher/e- safety leader and decide whether to inform parents of any children who viewed the site.

3. Inform the school technicians and ensure the site is filtered (LGfL schools report to: webalerts@synetrix.com).

- **An inappropriate website is accessed intentionally by a child.**

1. Refer to the acceptable use policy that was signed by the child, and apply agreed sanctions.

2. Notify the parents of the child.

3. Inform the school technicians and ensure the site is filtered if need be.

- **An adult uses School IT equipment inappropriately.**

1. Ensure you have a colleague with you; do not view the misuse alone.

2. Report the misuse immediately to the head teacher and ensure that there is no further access to the PC or laptop.

3. If the material is offensive but not illegal, the head teacher
4. should then:

- Remove the PC to a secure place.
- Instigate an audit of all ICT equipment by the schools ICTmanaged service providers to ensure there is no risk of pupils accessing inappropriate materials in the school.
- Identify the precise details of the material.
- Take appropriate disciplinary action (contact Personnel/Human Resources).
- Inform governors of the incident.
- In an extreme case where the material is of an illegal nature:
- Contact the local police and follow their advice.
- If requested to, remove the PC to a secure place and document what you have done.

- **A bullying incident directed at a child occurs through email or mobile phone technology, either inside or outside of school time.**

1. Advise the child not to respond to the message.
2. Refer to relevant policies including e-safety anti-bullying and PHSE and apply appropriate sanctions.
3. Secure and preserve any evidence.
4. Inform the sender's e-mail service provider.
5. Notify parents of the children involved.
6. Consider delivering a parent workshop for the school community.
7. Inform the police if necessary.

- **Malicious or threatening comments are posted on an Internet site about a pupil or member of staff.**

1. Inform and request the comments be removed if the site is administered externally.
2. Secure and preserve any evidence.
3. Send all the evidence to CEOP at www.ceop.gov.uk/contact_us.html.
4. Endeavour to trace the origin and inform police as appropriate.
5. Keep Head teacher informed at every development stage

The school may wish to consider delivering a parent workshop for the school community or issue a statement in newsletter

You are concerned that a child's safety is at risk because you suspect someone is using communication technologies (such as social networking sites) to make inappropriate contact with the child

1. Report to and discuss with the named safeguarding officer in school and contact parents.
2. Advise the child on how to terminate the communication and save all evidence.
3. Contact CEOP http://www.ceop.gov.uk/
4. Consider the involvement police and social services.
5. Consider delivering a parent workshop for the school community.

All of the above incidences must be reported immediately to the head teacher and online safety/ safeguarding leader.

All Children at Edinburgh should be confident in a no-blame culture when it comes to reporting inappropriate incidents involving the internet or mobile technology: they must be able to do this without fear.