Elmhurst Junior School Online Safety Policy 2020

This policy has been written by the Computing Lead at Elmhurst and shared with staff, children, parents and Governors .

It should be read in conjunction with the Child Protection and Safeguarding Policy and the Prevent Policy.

Contents

Appendices:

http://www.digitallyconfident.org/images/resources/first-line-information-support-HQ.pdf - page 23 onwards

6. Protocol for Data Security
7. Search and Confiscation guidance from DfE https://www.gov.uk/government/publications/searching-screening-and-confiscation

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 Elmhurst Junior School with respect to the use of ICT-based technologies.
- safeguard and protect the children and staff of Elmhurst Junior School.
- assist school staff working with children to work safely and responsibly with the Internet and other 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.
- have clear structures to deal with online abuse such as cyberbullying which are cross referenced with other school 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 school community can be summarised as follows:

Content

- exposure to inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence associated with often racist language)
- lifestyle websites, for example pro-anorexia/self-harm/suicide sites
- hate sites
- content validation: how to check authenticity and accuracy of online content

Contact

- grooming
- cyber-bullying in all forms
- identity theft (including 'frape' (hacking Facebook profiles)) and sharing passwords

Conduct

- privacy issues, including disclosure of personal information
- digital footprint and online reputation
- health and well-being (amount of time spent online (Internet or gaming))
- sexting (sending and receiving of personally intimate images) also referred to as SGII (self-generated indecent images)
- copyright (little care or consideration for intellectual property and ownership – such as music and film)

Scope (from LGfL)

This policy applies to all members of Elmhurst Junior School community (including staff, pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of Elmhurst Junior School.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the *school* site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data (see appendix for template policy). In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.

Role	Key Responsibilities
Headteacher	● To take overall responsibility for online safety provision ● To take overall responsibility for data and data security (SIRO) ● To ensure the school uses an approved, filtered Internet Service, which complies with current statutory requirements e.g.SWGfL ● To be responsible for ensuring that staff receive suitable training to carry out their online safety roles and to train other colleagues, as relevant ● To be aware of procedures to be followed in the event of a serious e-safety incident ● To receive regular filtering reports ● 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)

Designated Child Protection Lead (ML) - with support from the Safeguarding team	● takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents ● promotes an awareness and commitment to online safeguarding throughout the school community ● ensures that online safety education is embedded across the curriculum ● liaises with school computing technical staff ● To communicate regularly with SLT and the designated e-safety/safeguarding 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 staff are using CPOMS to log any online safety incidents ● facilitates training and advice for all staff ● liaises 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 issues to arise from: • sharing of personal data • access to illegal / inappropriate materials • inappropriate on-line contact with adults / strangers • potential or actual incidents of grooming • cyber-bullying and use of social media
Governors	● To ensure that the school follows all current online safety advice to keep the children and staff safe ● To approve the Online Safety Policy and review the effectiveness of the policy. This will be carried out by the Governors receiving regular information about online safety incidents and monitoring reports. ● To support the school in encouraging parents and the wider community to become engaged in online safety activities
Leader of Computing (SR)	● To oversee the delivery of the online safety element of the Computing curriculum ● To liaise with the Headteacher regularly
Network Manager (ML/NR)	● To report any online safety related issues that arises, to the Leader of Computing ● To ensure that users may only access the school's networks through an authorised and properly enforced password protection policy, in which passwords are regularly changed ● To ensure that provision exists for misuse detection and malicious attack e.g. keeping virus protection up to date ● To ensure the security of the school ICT system ● To ensure that access controls / encryption exist to protect personal and sensitive information held on school-owned devices • To ensure that the school's policy on web filtering is applied and updated on a regular basis • SWGfL is informed of issues relating to the filtering applied by the Grid

	• that he / she keeps 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 the network / Google Apps for Education / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Computing lead /Headteacher for investigation, action or sanction ● To ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster. ● To keep up-to-date documentation of the school's e-security and technical procedures
Data Manager/ Headteacher	● To ensure that all data held on pupils on the server, SIMs or Google Apps for Education domain is adequately protected ● To ensure that all data held on pupils on the school office machines have appropriate access controls in place ● To ensure all SWGfL services are managed on behalf of the school
Teachers	● To embed online safety issues in all aspects of the curriculum and other school activities ● 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 and help promote the school's online safety policies and guidance ● To read, understand, sign and adhere to the school staff Acceptable Use Agreement / Policy ● To be aware of online safety issues related to the use of mobile phones, cameras and handheld devices and that they monitor their use and implement current school policies with regard to these devices ● To report any suspected misuse or problem to the online safety/computing lead or 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 ● To ensure that any digital communications with pupils should be on a professional level and only through school based systems, never through personal mechanisms, e.g. email, text, mobile phones etc.
Pupils	● To read, understand, sign and adhere to the Student / Pupil Acceptable Use Policy ● 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 know and understand school policy on the use of mobile phones, digital cameras and handheld devices.

	● To know and understand school policy on the taking / use of images and on cyber-bullying. ● To understand the importance of adopting 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, if related to their membership of the school ● To take responsibility for learning about the benefits and risks of using the Internet and other technologies safely both in school and at home ● To help the school in the creation/ review of online safety policies
Parents/carers	● To support the school in promoting online safety and endorse the Parents' Acceptable Use Agreement which includes the pupils' use of the Internet and the school's use of photographic and video images ● To read, understand and promote the school Pupil Acceptable Use Agreement with their children ● To access the school website and newsletter for regular online safety updates and useful website links ● To consult with the school if they have any concerns about their children's use of technology
External groups	● Any external individual / organisation will sign an Acceptable Use Policy prior to using any equipment or the Internet within school

Communication:

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

- Policy to be posted on the school website and the staffroom display
- A link to the policy is included in the online staff handbook
- Acceptable use agreements discussed with pupils at the start of each year.
- Acceptable use agreements to be issued to the whole school community, usually on entry to the school
- Acceptable use agreements to be held in pupil and personnel files within the office

Handling complaints:

- The school will take all reasonable precautions to ensure online safety. However, 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.

- Staff and pupils are given information about infringements in use and possible sanctions. Sanctions available include:
    - interview/counselling by teacher /Year leader/ computing lead / Headteacher;
    - informing parents or carers;
    - removal of Internet or computer access for a period, [which could ultimately prevent access to files held on the system];
    - referral to LA / Police.

- Our online safety/computing lead acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the Headteacher in the first instance.

- Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with school / LA child protection procedures.

Review and Monitoring

The online safety policy is referenced from within other school policies: online safety policy, Child Protection policy, Anti-Bullying policy and in the School Development Plan, Behaviour policy, Personal, Social and Health Education.

- The school has an online safety lead (The Leader of computing) who will be responsible for document ownership, review and updates.
- The online safety policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the school
- The online safety policy has been written by the Lead of computing and is current and appropriate for its intended audience and purpose.
- 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 safeguarding policy will be discussed in detail with all members of teaching staff.

Version Control

As part of the maintenance involved with ensuring our online safety policy is updated, revisions will be made to the document. It is important that the document owner ensures the document contains the following information and that all revisions are stored centrally for audit purposes.

Title	Elmhurst Junior School online safety policy
Version	0.4
Date	2/09/2019
Author	Computing lead
Approved by head teacher	T.Edwards/ M.Lawrence
Approved by Governing Body	
Next Review Date	Autumn 2020

Modification History			
Version	Date	Description	Revision Author
0.1	12/09/2013	Initial draft	e-safety coordinator
0.2	06/03/2015	Updated draft	E-safety coordinator
0.3	27/09/2017	Updated	Online safety/computing lead
0.4	2/09/2019	updated	Online safety/computing lead
0.5	19/10/2020	Current version	Online saftey/computing lead

2. Education and Curriculum

Pupil online safety curriculum

This school

- Has a clear, progressive online safety education programme as part of the Computing curriculum / PSHE curriculum. It is built on The Somerset Elim lesson plans. This covers a range of skills and behaviours appropriate to their age and experience, including:
    - to STOP and THINK before they CLICK
    - to develop a range of strategies to evaluate and verify information before accepting its accuracy;
    - to be aware that the author of a web site / page may have a particular bias or purpose and to develop skills to recognise what that may be;
    - to know how to narrow down or refine a search;
    - [for older pupils] to understand how search engines work and to understand that this affects the results they see at the top of the listings;
    - to understand acceptable behaviour when using an online environment / email, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private;
    - to understand how photographs can be manipulated and how web content can attract the wrong sort of attention;
    - to understand why on-line 'friends' may not be who they say they are and to understand why they should be careful in online environments;
    - to understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have turned-on privacy settings;
    - to understand why they must not post pictures or videos of others without their permission;
    - to know not to download any files – such as music files - without permission;
    - to have strategies for dealing with receipt of inappropriate materials;
    - [for older pupils] to understand why and how some people will 'groom' young people for sexual reasons;
    - To understand the impact of cyberbullying, sexting and trolling and know how to seek help if they are affected by any form of online bullying.
    - To know how to report any abuse including cyberbullying; and how to seek help if they experience problems when using the Internet and related technologies, i.e. parent or carer, teacher or trusted staff member, or an organisation such as ChildLine or the CLICK CEOP button.

- Plans Internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas. The Elim plans allow for progression from Year 3 to Year 6
- Will remind students about their responsibilities through an Acceptable Use Policy which every student will sign and will be reminded of when using school equipment.
- Ensures staff will model safe and responsible behaviour in their own use of technology during lessons.
- Ensures that when copying materials from the web, staff and pupils understand issues around plagiarism; how to check the copyright and also know that they must respect and acknowledge copyright / intellectual property rights;

- Ensures that staff and pupils understand the issues around aspects of the commercial use of the Internet, as age appropriate. This may include, risks in pop-ups; buying on-line; on-line gaming / gambling;

Staff and governor training

This school

- Ensures staff know how to send or receive sensitive and personal data and understand the requirement to encrypt data where the sensitivity requires data protection;
- Makes regular training available to staff on e-safety issues and the school's e-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 e-safeguarding policy and the school's Acceptable Use Policies.
- Uses CPOMS to record and log any online safety incidents (Headteacher, safeguarding lead and computing lead are instantly notified)

Parent awareness and training

This school

- Runs a rolling programme of advice, guidance and training for parents, including:
    - Introduction of the Acceptable Use Agreements to new parents, to ensure that principles of online safety behaviour are made clear
    - Information leaflets; in school newsletters; on the school website;
    - demonstrations, practical sessions held at school e.g. Family Learning Afternoon;
    - suggestions for safe Internet use at home;
    - provision of information about national support sites for parents.

3. Expected Conduct and Incident management

Expected conduct

In this school, all users:

- are responsible for using the school computing systems in accordance with the relevant Acceptable Use Policy which they will be expected to sign before being given access to school systems.
- need to understand the importance of misuse or access to inappropriate materials and are aware of the consequences
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- should understand the importance of adopting good online practice when using equipment out of school and realise that the school's online safety policy covers their actions out of school, if related to their membership of the school
- will be expected to know and understand school policies on the use of mobile phones, digital cameras and handheld devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying

Staff

- are responsible for reading the school's online safety policy and using the school ICT systems accordingly, including the use of mobile phones, and handheld devices.

Students/Pupils

- should have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations

Parents/Carers

- should provide consent for pupils to use the Internet, as well as other technologies, as part of the online acceptable use agreement form at time of their child's entry to the school
- should know and understand what the 'rules of appropriate use' 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, though the attitudes and behaviour of users are generally positive and there is rarely need to apply sanctions
- all members and its wider community 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 (e.g. the local authority and regional broadband grid, UK Safer Internet Centre helpline) 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. The records are reviewed/audited and reported to the school's senior leaders, Governors /the LA
- parents / carers are specifically informed of online safety incidents involving young people for whom they are responsible.

- We will contact the Police if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law

4. Managing the ICT infrastructure

- **Internet access, security (virus protection) and filtering**

This school:

- Has the educational filtered secure broadband connectivity through the SWGfL and also connects to the 'private' Google Apps for Education domain;
- Uses the SWGfL Net Sweeper filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature, etc. All changes to the filtering policy is logged and only available to staff with the approved 'web filtering management' status;
- Ensures networks remain healthy through use of Sophos anti-virus software (from SWGfL) etc. and network set-up so staff and pupils cannot download executable files;
- Uses DfE, LA, Google Apps for Education domain or SWGfL approved secured email to send personal data over the Internet and uses encrypted devices, secure remote access or Google Apps for Education where staff need to access personal level data off-site;
- Blocks all Chat rooms and social networking sites except those that are part of an educational network or approved Learning Platform;
- Only unblock other external social networking sites for specific purposes / Internet Literacy lessons;
- Has blocked pupil access to music download or shopping sites – except those approved for educational purposes at a regional or national level;
- Uses security time-outs on Internet access where practicable / useful;
- Works in partnership with the SWGfL to ensure any concerns about the system are communicated so that systems remain robust and protect students;
- Ensures all staff and students have signed an acceptable use agreement form and understands that they must report any concerns;
- Ensures pupils only publish within an appropriately secure environment : the school's learning environment/ the school Google Apps for Education domain;
- Requires staff to preview websites before use [where not previously viewed or cached] and encourages use of the school's Learning Platform as a key way to direct students to age / subject appropriate web sites; Plans the curriculum context for Internet use to match pupils' ability/age, using child-friendly search engines where more open Internet searching is required; e.g. yahoo for kids or ask for kids , Google Safe Search , …..
- Is vigilant when conducting 'raw' image search with pupils e.g. Google image search;
- Informs all users that Internet use is monitored;
- Informs staff and students that they must report any failure of the filtering systems directly to the Computing Lead. Our Computing Lead logs or escalates as appropriate to the Technical service provider or SWGfL Helpdesk as necessary;

- Makes clear all users know and understand what the 'rules of appropriate use' are and what sanctions result from misuse – through staff meetings and teaching programme;
- Provides advice and information on reporting offensive materials, abuse/ bullying etc. available for pupils, staff and parents
- Immediately refers any material we suspect is illegal to the appropriate authorities – Police – and the LA.

- **Network management (user access, backup)**
  This school
  - Uses individual, audited log-ins for all users – SWGFL or Google Apps for Education;
  - 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 SWGfL services and policies / requires the Technical Support Provider to be up-to-date with SWGfL services and policies;
  - Storage of all data within the school will conform to the UK data protection requirements

    Pupils and Staff using mobile technology, where storage of data is online, will conform to the General Data Protection Regulation,where storage is hosted within the EU or protected under the Safe Harbouring Scheme.

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;
- Staff access to the schools' management information system is controlled through a separate password for data security purposes;
- We provide pupils with an individual Google Apps for Education network log-in username. From Year 3 they are also expected to use a personal password. This password can only be changed by an administrator e.g. Computing Lead or Headteacher;
- All pupils have their own unique username and password which gives them access to the Internet, the Google Apps for Education Learning Platform and their own school approved email account;
- 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 as these have far less security restrictions and inappropriate use could damage files or the network;
- 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 always log off/lock computers when they have finished working or are leaving the computer unattended;

- Where a user finds a logged-on machine, we require them to always log-off and then log-on again as themselves
- Requests that teachers and pupils do not switch the computers off during the day unless they are unlikely to be used again that day or have completely crashed. We request that they DO switch the computers off at the end of the day;
- Has set-up the network so that users cannot download executable files / programmes;
- Has blocked access to music/media download or shopping sites – except those approved for educational purposes;
- Scans all mobile equipment with anti-virus / spyware before it is connected to the network;
- Makes clear that staff are responsible for ensuring that all equipment that goes home has the anti-virus and spyware software maintained up-to-date and the school provides them with a solution to do so;
- Makes clear that staff are responsible for ensuring that any computer or laptop loaned to them by the school, is used solely to support their professional responsibilities and that they notify the school of any "significant personal use" as defined by HM Revenue & Customs.
- *Makes clear that staff accessing LA systems do so in accordance with any Corporate policies;*
  e.g. County email or Intranet; finance system, Personnel system etc.
- Maintains equipment to ensure Health and Safety is followed;
  e.g. projector filters cleaned by site manager / ICT Support; equipment installed and checked by approved Suppliers / LA electrical engineers
- Has integrated curriculum and administration networks, but access to the Management Information System is set-up so as to ensure staff users can only access modules related to their role;
  e.g. teachers access report writing module; SEN coordinator - SEN data;
- Ensures that access to the school's network resources from remote locations by staff is 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 restricted and is only through approved systems;
  e.g. technical support or SIMs Support, our Education Welfare Officers accessing attendance data on specific children;
- Provides pupils and staff with access to content and resources through the school domain or Google Apps for Education domain which staff and pupils access using their username and password;
- Makes clear responsibilities for the daily back up of SIMs and finance systems and other important files;
- Has a clear disaster recovery system in place for critical data that includes a secure, on site and offsite remote backup of critical data, that complies with external Audit's requirements;
- 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;

- Follows ISP advice on Local Area and Wide Area security matters and firewalls and routers have been configured to prevent unauthorised use of our network;
- Our wireless network has been secured to industry standard Enterprise security level /appropriate standards suitable for educational use;
- All computer equipment is installed professionally and meets health and safety standards;
- Projectors are maintained so that the quality of presentation remains high;
- Reviews the school ICT systems regularly with regard to health and safety and security.

Password policy

- This school makes it clear that staff and pupils must always keep their password private, must not share it with others and must not leave it where others can find it;
- All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password private.
- We require staff to use a minimum 8 digit password including a capital and number to log into our school systems.
- We require staff to change their passwords into the school domain every 30 days.

E-mail

This school

- Provides staff with an email account for their professional use, *(LA email and Google Apps for Education email)* and makes clear personal email should be through a separate account;
- Uses Google Apps for Education email with students as this has email content control
- Does not publish personal home e-mail addresses of pupils or staff on the school website. We use school-based emails for communication with the wider public.
- 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
- Reports messages relating to or in support of illegal activities to the relevant Authority and if necessary to the Police.
- Knows that spam, phishing and virus attachments can make emails dangerous. We use a number of SWGfL and Google Apps-provided technologies to help protect users and systems in the school, including desktop anti-virus product Sophos, plus direct email filtering for viruses, Trojans, pornography, phishing and inappropriate language.

Pupils:

- We use Google Apps for Education email with pupils and lock this down where appropriate..

  Pupils are introduced to, and use email as part of the Computing scheme of work.

- Pupils can only send and receive mail to and from within the Google Apps for Education school domain.

- Pupils use Google classroom to complete work that is set by the class teacher both at home and in school. This is especially important during any future school closures e.g. due to pandemics such as COVID19. Provisions will be made if any child has no access to computers/internet at home. Pupils are aware of appropriate use of Google classroom and how to share.hand in their work to their teacher.

- Pupils are taught about the safety and 'netiquette' of using email both in school and at home i.e. they are taught:

  - not to give out their email address unless it is part of a school managed project or to someone they know and trust and is approved by their teacher or parent/carer;
  - that an email is a form of publishing where the message should be clear, short and concise;
  - that any email sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper;
  - they must not reveal private details of themselves or others in email, such as address, telephone number, etc.;
  - to 'Stop and Think Before They Click' and not open attachments unless sure the source is safe;
  - that they should think carefully before sending any attachments;
  - embedding adverts is not allowed;
  - that they must immediately tell a teacher / responsible adult / computing comrade if they receive an email which makes them feel uncomfortable, is offensive or bullying in nature;
  - not to respond to malicious or threatening messages;
  - not to delete malicious of threatening emails, but to keep them as evidence of bullying;
  - not to arrange to meet anyone they meet through email without having discussed with an adult and taking a responsible adult with them;
  - that forwarding 'chain' email letters is not permitted.

- Pupils sign the school Agreement Form to say they have read and understood the online safety rules, including email and we explain how any inappropriate use will be dealt with.

Staff:

- Staff only use LA or Google Apps for Education email systems for professional purposes.

- Staff know that emails sent to an external organisation must be written carefully, (and may require authorisation), in the same way as a letter written on school headed paper.

- All staff sign our School Agreement Form to say they have read and understood the online safety rules, including email and we explain how any inappropriate use will be dealt with.

School website

- The Headteacher takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained;
- Uploading of information is restricted to our website authorisers: <e.g. The headteachers
- The school website complies with the statutory DfE guidelines for publications;
- 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;
- The point of contact on the web site is the school address, telephone number and we use a general email contact address, e.g. office@elmhurst.sch.somerset.gov.uk. Home information will not be published;
- 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;
- We do not use embedded geodata in respect of stored images;
- We expect teachers using' school approved blogs or wikis to password protect them and run from the school website.

Learning platform

- Uploading of information on the schools' Google Apps for Education domain is shared between different staff members according to their responsibilities e.g. all class teachers upload information in their class areas. Google classroom is used in order to provide blended learning opportunites. Homework is often set on Google classroom and in the case of a school closure, classwork can be set via Google Classroom.
- Photographs and videos uploaded to the schools domain or the schools Google Apps for Education domain will only be accessible by members of the school community;
- In school, pupils are only able to upload and publish within school approved and closed systems, such as the school domain or the school Google Apps for Education domain;

Social networking

- 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 e.g. class dojo, google classroom;
- The school's preferred system for social networking will be maintained in adherence with the communications policy.

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 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
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Video Conferencing

This school

- Only uses Google Apps for Education video conferencing activity;

CCTV

- We have CCTV in the school as part of our site surveillance for staff and student safety. We will not reveal any recordings (*retained by the Support Provider for 28 days*), without permission except where disclosed to the Police as part of a criminal investigation.
- We use specialist lesson recording equipment on occasions as a tool to share best teaching practice. We do not reveal any such recordings outside of the staff and will not use for any other purposes.

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 in a spreadsheet.
  https://docs.google.com/document/d/1FBHmlRLU_TSMBIxxfwgSS8Vl8s6bLDTNQtK8scXgHqc/edit
- 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 one central record <in *name of MIS* e.g. SIMS, Progresso etc., Personnel or spreadsheet>.

  We ensure ALL the following school stakeholders sign an Acceptable Use Agreement form. We have a system so we know who has signed.

  - staff,
  - governors,
  - pupils
  - parents

  This makes clear staff responsibilities with regard to data security, passwords and access.
- We follow LA guidelines for the transfer of any data, such as SIMs data or reports of children, to professionals working in the Local Authority or their partners in Children's Services / Family Services, Health, Welfare and Social Services.
- We require that any Protected and Restricted material must be encrypted if the material is to be removed from the school or the school domain (such as Google Apps for Education) and limit such data removal. / We have an approved remote access and an approved Google Apps for Education solution so staff can access sensitive and other data from home, without the need to take data home.
- School staff with access to setting-up usernames and passwords for email, network access and Google Apps for Education access are working within the approved system and follow the security processes required by those systems.
- We ask staff to undertake at least annual house-keeping to review, remove and destroy any digital materials and documents which need no longer be stored.
- Photographs are deleted from ipads termly.

Technical Solutions

- Staff have secure area(s) on the network to store sensitive documents
- We require staff to log-out of systems when leaving their computer, but also enforce lock-out after 10 minutes idle time.
- We use Google Apps for Education to prevent any member of staff from having to take any sensitive information off site.

- We store any Protect and Restricted written material in lockable storage cabinets in a lockable storage area.
- All servers are in lockable and alarmed locations and managed by DBS-checked staff.
- We use Gigasoft remote secure back-up for disaster recovery on our admin, and curriculum server.
- We comply with the WEEE directive on equipment disposal by using an approved or recommended disposal company for disposal of equipment where any protected or restricted data has been held and get a certificate of secure deletion for any server or PC that once contained personal data.
- Portable equipment (such as ipads and laptops) loaned by the school (for use by staff at home), where used for any protected data, is disposed of through the same procedure.
- Paper based sensitive information is shredded, using cross cut shredder or sent for external safe disposal.

6. Equipment and Digital Content

Staff ipads

- Staff ipads are provided to allow access to school LA and Google Apps for Education email, 'Drive' and calendar accounts. All staff ipads must have the lock screen pin code activated and auto lock in 5 minutes or less of inactivity. Find my ipad and location services must be activated so the ipads can be found, locked or wiped should they be lost.

Personal mobile phones and mobile devices

- Mobile phones brought into school are entirely at the staff member, student's & parents' or visitors own risk. The School accepts no responsibility for the loss, theft or damage of any phone or handheld device brought into school.
- Student mobile phones which are brought into school must be turned off (not placed on silent) and given to the teacher. They must remain turned off and out of sight until the end of the day. Staff members may use their phones during school break times in designated areas such as the staffroom.
- All visitors are requested to keep their phones on silent and kept away. There is a sign indicating no use of mobiles on entrance to school via the main office.
- The recording, taking and sharing of images, video and audio on any mobile phone is to be avoided; except where it has been explicitly agreed otherwise by the Headteacher. Such authorised use is to be monitored and recorded. All mobile phone use is to be open to scrutiny and the Headteacher is to be able to withdraw or restrict authorisation for use at any time if it is to be deemed necessary.
- The School reserves the right to search the content of any mobile or handheld devices on the school premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying. Staff mobiles or hand held devices may be searched at any time as part of routine monitoring.
- Where parents or students need to contact each other during the school day, they should do so only through the School's telephone. 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.
- Mobile phones and personally-owned devices will not be used in any way during lessons or formal school time. They should be switched off or silent at all times.
- Mobile phones and personally-owned mobile devices brought into school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally-owned mobile phones or mobile devices.
- Mobile phones and personally-owned devices are not permitted to be used in certain areas within the school site, e.g. changing rooms and toilets.
- Mobile phones will not be used during lessons or formal school time unless as part of an approved and directed curriculum-based activity with consent from a member of staff.
- The Bluetooth or similar function of a mobile phone should be switched off at all times and not be used to send images or files to other mobile phones.

- Personal mobile phones will only be used during lessons with permission from the headteacher.
- No images or videos should be taken on mobile phones or personally-owned mobile devices without the prior consent of the person or people concerned.
-

Students' use of personal devices

- The School strongly advises that student mobile phones should not be brought into school.
- The School accepts that there may be particular circumstances in which a parent wishes their child to have a mobile phone for their own safety.
- All mobile phones and personally-owned devices will be handed into the teacher in the classroom should they be brought into school and will be kept out of reach.
- If a student breaches the school policy then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents or carers in accordance with the school policy.
- Phones and devices must not be taken into examinations. Students found in possession of a mobile phone during an exam will be reported to the appropriate examining body. This may result in the student's withdrawal from either that examination or all examinations.
- 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.
- 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.

Staff use of personal devices

- Any permitted images or files taken in school must be downloaded from the device and deleted in school before the end of the day.
- Staff are not permitted to use their own mobile phones or devices for contacting children, young people or their families within or outside of the setting in a professional capacity.
- Staff will have access to a school phone where contact with students, parents or carers is required when offsite during the school day unless using 141 on their own devices
- Mobile Phones and personally-owned devices will be switched off or switched to 'silent' mode. Mobile phones or personally-owned devices will not be used during teaching periods unless permission has been granted by the Headteacher.
- If members of staff have an educational reason to allow children to use mobile phones or a personally-owned device as part of an educational activity then it will only take place when approved by the senior leadership team.
- Staff should not use personally-owned devices, such as mobile phones or cameras, to take photos or videos of students and will only use work-provided equipment for this

purpose. Where work-provided equipment is not available, permission should be sought to take photos and video on personal devices and all photos and videos should be deleted from personal devices before leaving the school site.

- If a member of staff breaches the school policy then disciplinary action may be taken.
- Where staff members are required to use a mobile phone for school duties, for instance in case of emergency during off-site activities, or for contacting students or parents, then a school mobile phone will be provided and used. 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.
- LA school and Google Apps for Education email and 'Drive' accounts can be installed on personal mobile phones but are subject to security restrictions set by the administrator, including screen pin lock code and automatic screen lock after 5 minutes, allowing the administrator access to lock the phone, change the pin and wipe the phone should it be required.

Digital images and video
In this school:

- 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 obtains parental permission for pictures and videos via an opt in/opt out policy at the start of a students entry to Elmhurst and this will allow photos and videos to be used on the school website, in the prospectus or in other high profile publications.
- The school blocks/filters access to social networking sites or newsgroups unless there is a specific approved educational purpose;
- Pupils are taught about how images can be manipulated in their online safety education programme and are 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, such as house number, street name or school. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

Asset disposal

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.
All redundant equipment will be disposed of through an authorised agency. This will include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.

All redundant equipment that may have held personal data will have the storage media forensically wiped. Alternatively, if the storage media has failed, it will be physically destroyed. The school will only use authorised companies who will supply a written guarantee that this will happen

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.