Cromwell High School

E-Safety Policy

Status: Active Date: Feb 2021 Review Next Date: 2023

Governor Leadership: Chair of Finance, Resources and Health and Safety Committee
Executive Leadership: Headteacher
Key Manager: Assistant Head Teacher
Consultation/signing group: Personal Growth and Wellbeing.

What the pupils need to know:

- We will always follow the school's 3Ts for internet safety.
- We will never give out personal information.
- We will never use digital equipment in school that they have brought in from home.

What every member of staff needs to know:

- We will maintain high levels of supervision and stop any child that is accessing inappropriate materials.
- We will follow the school's code of conduct, especially around social media and its uses.
- We will never share or ask for personal information from any of the children in school.

What every adult needs to know:

- Cromwell High School will not tolerate anyone accessing inappropriate materials on site.
- Asking children for contact information.
- Sharing images or clips on social media of the children in Cromwell, unless it's solely of their own child.

Procedures:
Two yearly- Personal Growth and Wellbeing review.

Monitoring and Management:
Computing and /or Wellbeing lead to review on a two yearly basis.

CROMWELL HIGH SCHOOL COMPUTER/E-SAFETY POLICY

Learning today, for a better

tomorrow.

Date reviewed by the Health and Safety Committee: May 2019

CONTENTS

1. Introduction and Overview

Rationale and Scope

The purpose of this policy is to:

- set out the key principles expected of all members of the school community at Cromwell High School with respect to the use of ICT-based technologies.
- to safeguard and protect the children and staff of Cromwell High 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 in place to deal with online abuse, such as cyberbullying, grooming, radicalization or exposure to harmful content, 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), substance abuse.
- Lifestyle websites, for example pro-anorexia/self-harm/suicide sites.
- Hate sites.
- Sites that prompt radicalisation.
- Children putting themselves at risks of CSE.
- Children carrying out acts (intentionally or unintentionally) that break the law, these include online piracy and behaviours that would be deemed to be CSE.
- Content validation: how to check authenticity and accuracy of online content.
- Children sharing and sending inappropriate information, media content or any such materials that result in distress to another child.

Contact

- Grooming.
- Cyberbullying 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).

This policy applies to all members of Cromwell High School community (including staff, students/pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of Cromwell High 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 cyberbullying, 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 regards to the searching for and of electronic devices and the deletion of data. 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
Head of school / Headteacher / Behaviour and safety leader / Business manager	• To take overall responsibility for e-safety provision • To take overall responsibility for data and data security (SIRO) / (GDPR) • To ensure the school uses an approved, filtered Internet Service, which complies with current statutory requirements • To be responsible for ensuring that staff receive suitable training to carry out their e-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 monitoring reports from the E-Safety Coordinator / Officer • To ensure that there is a system in place to monitor and support staff who carry out internal e-safety procedures (e.g. network manager)

Behaviour and safety lead / Designated Child Protection Lead	• Takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies/documents
	• Promotes an awareness and commitment to e-safeguarding throughout the school community
	• Ensures that e-safety education is embedded across the curriculum
	• Liaises with school ICT technical staff
	• To communicate regularly with SLT and the designated e-safety Governor / committee to discuss current issues, review incident logs and filtering / change control logs
	• To ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident
	• To ensure that an e-safety incident log is kept up to date
	• Facilitates training and advice for all staff
	• Liaises with the Local Authority and relevant agencies
	• Is regularly updated in e-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
	  • cyberbullying and use of social media

Governors / E-safety (Health and safety governor)	• To ensure that the school follows all current e-safety advice to keep the children and staff safe • To approve the E-Safety Policy and review the effectiveness of the policy. This will be carried out by the Governors / Governors Sub- Committee receiving regular information about e-safety incidents and monitoring reports. A member of the Governing Body has taken on the role of E-Safety Governor • To support the school in encouraging parents and the wider community to become engaged in e-safety activities • The role of the E-Safety Governor will include regular review with the E-Safety Coordinator / Officer (including e-safety incident logs, filtering / change control logs)

Role	Key Responsibilities
Computing Curriculum Leader	• To oversee the delivery of the e-safety element of the Computing curriculum • To liaise with the e-safety coordinator regularly
Network Manager/ technician	• To report any e-safety related issues that arises, to the e-safety coordinator • 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 • The school's policy on web filtering is applied and updated on a regular basis • LGfL is informed of issues relating to the filtering applied by the Grid • That he/she keeps up to date with the school's e-safety policy and technical information in order to effectively carry out their e-safety role and to inform and update others as relevant • That the use of the *network / Virtual Learning Environment (LEARNING PLATFORM) / remote access / email* is regularly monitored in order that any misuse / attempted misuse can be reported to the *E-Safety Co-ordinator / Officer /Headteacher for investigation / action / 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
Learning platform.	• To ensure that all data held on pupils on the LEARNING PLATFORM is adequately protected
Data Manager	• To ensure that all data held on pupils on the school office machines have appropriate access controls in place
Teachers	• To embed e-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

Role	Key Responsibilities
All staff	• To read, understand and help promote the school's e-safety policies and guidance • To read, understand, sign and adhere to the school Staff Acceptable Use Agreement / Policy • To be aware of e-safety issues related to the use of mobile phones, cameras and hand held 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 e-safety coordinator • To maintain an awareness of current e-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	• Read, understand, sign and adhere to the Student / Pupil Acceptable Use Policy (NB: at KS1, it would be expected that parents/carers would sign on behalf of the pupils) • Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations • 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 hand held devices. • To know and understand school policy on the taking/use of images and on cyberbullying. • To understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-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 e-safety policies
Parents/carers	• To support the school in promoting e-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 / LEARNING PLATFORM / online student/pupil records in accordance with the relevant school Acceptable Use Agreement.

Role	Key Responsibilities
	• 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/staffroom/classrooms
- Policy to be part of school induction pack for new staff
- Acceptable use agreements discussed with pupils at the start of each year
- Acceptable use agreements to be issued to whole school community, usually on entry to the school
- Acceptable use agreements to be held in pupil and personnel files

Handling complaints:

- The school will take all reasonable precautions to ensure e-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 tutor / Head of department / E-Safety Coordinator / 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, including examination coursework];
    - All hand-held devices to be locked away on arrival;
    - referral to LA / Police.

- Our E-Safety Coordinator acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the Headteacher.

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

- The school has a Computing coordinator who will be responsible for document ownership, review and updates.
- The E-Safety policy will be reviewed every two years or when any significant changes occur with regard to the technologies in use within the school.
- The E-Safety policy has been written by the school ICT Coordinator 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 and other stakeholders such as the PTA. All amendments to the school e-safeguarding policy will be discussed in detail with all members of teaching staff.

2. Education and Curriculum

Pupil *e*-safety curriculum

This school:

- Has a clear, progressive e-safety education programme as part of the Computing curriculum/PSHCE curriculum. 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 website/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, gaming, communication apps, 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 online '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 understand that they must not post anything online that is harmful to others or request another person do something inappropriate;
    - 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.
- Plan Internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.
- Will remind students about their responsibilities through an end-user Acceptable Use Policy which every student will sign/will be displayed throughout the school/will be displayed when a student logs on to the school network.
- Ensures staff will model safe and responsible behaviour in their own use of technology during lessons.
- *All children will learn about staying safe when using 'Teams' or any other such online video service for learning or personal use. (Refer to the school's Home learning agreement for 'Teams.'*

- Ensures that when copying materials from the web, staff and pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright/intellectual property rights;

ASC children and modification of approach and delivery

All reasonable adjustments will be made for our ASC children, with each and every child being taught the skills that will help to keep them safe online and ensure the safety of others.

Where ICT is used as a motivating reward, it will be monitored carefully:

- 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 online; on-line gaming; gambling; sexually explicit content.

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; annual updates/termly staff meetings, etc.
- 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.

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 e-safe behaviour are made clear;
    - Information leaflets; in school newsletters; on the school website;
    - demonstrations, practical sessions held at school;
    - 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 ICT systems in accordance with the relevant Acceptable Use Policy, which they will be expected to sign before being given access to school systems (at KS1 it would be expected that parents/carers would sign on behalf of the pupils);
- 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 e-safety practice when using digital technologies out of school and realise that the school's E-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 hand held 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 E-Safety policy and using the school ICT systems accordingly, including the use of mobile phones, and hand held 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 e-safety 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 E-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 e-safety issues;

- monitoring and reporting of e-safety incidents takes place and contribute to developments in policy and practice in e-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 e-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:

- Ensures network healthy through use of anti-virus software and network set-up, so staff and pupils cannot download executable files;
- Blocks all Chatrooms and social networking sites, except those that are part of an educational network or approved Learning Platform;
- Only unblocks other external social networking sites for specific purposes/Internet Literacy lessons;
- Has blocked all access to music download or shopping sites – except those approved for educational purposes at a regional or national level, such as Audio Network;
- Is vigilant in its supervision of pupils' use at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas where older pupils have more flexible access;
- Ensures all staff and students have signed an acceptable user agreement form and understands that they must report any concerns;
- Requires staff to preview websites before use [where not previously viewed or cached].
- Plans the curriculum context for Internet use to match pupils' ability, using child-friendly search engines where more open Internet searching is required; e.g. Google that is filtered with the school's web filter 'Light speed';
- High levels of vigilance 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 that they must report any failure of the filtering systems directly to the [system administrator/teacher/person responsible for URL filtering]. Our system administrator(s) logs or escalates as appropriate to the Technical service provider 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 guest accounts occasionally for external or short-term visitors for temporary access to appropriate services;
- Uses teacher 'remote' management control tools for controlling workstations / viewing users / setting-up applications and Internet web sites, where useful;
- Has additional local network auditing software installed;
- 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 EU data protection directive where storage is hosted within the EU.

The school takes all reasonable steps to ensure that any and all data and personal information on children and staff is held in accordance with the current GDPR regulations which came into effect in May 2018. Currently, Ali Syed is overseeing this and has attended the relevant training to ensure the school's compliance with the new regulations.

Any and all external providers that the school uses such as SIMS, BlueSky and CPOMS are all GDPR accredited.

To ensure the network is used safely, this school:

- Ensures staff read and sign that they have understood the school's E-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/use the same username and password for access to our school's network;
- 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 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. Borough 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/TA; 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, e.g. teachers access their area / a staff shared area for planning documentation via a VPN solution / RAv3 system;
- 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;
- All computer equipment is installed professionally and meets health and safety standards;
- Reviews the school ICT systems regularly with regard to health and safety and security.

Password policy

- This school makes it clear that staff 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.

E-mail

This school

- Provides staff with an email account for their professional use and makes clear personal email should be through a separate account;
- 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 technologies to help protect users and systems in the school, including a desktop anti-virus product.

Staff:

- Staff only use School e-mail systems for professional purposes;
- Access in school to external personal email accounts may be blocked;
- Staff know that e-mail 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. That it should follow the school 'house-style':
    - the sending of multiple or large attachments should be limited, and may also be restricted by the provider of the service being used;

- the sending of chain letters is not permitted;
- embedding adverts is not allowed;

- All staff sign our school Agreement Form to say they have read and understood the e-safety rules, including e-mail 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;
- The school web site 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;
- 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.

Social networking

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/academy or local authority;
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Online learning

School staff will ensure that during any form of online learning:

That all sessions have an adult in attendance to supervise the content being accessed or delivered, who will stop the session if needed. (Example- unaccepted user joins the session etc)

That children will only access sessions with services and providers that the school has fully vetted.

When sessions are being accessed by home learners, that only children with the relevant permission are on screen. This will result in some classes having to deactivate their cameras during some sessions.

That staff will turn off cameras and microphones should a child go into crisis or need medical support.

That staff will always adopt a high standard of professional communication during any online sessions.

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;
- We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials/DVDs;
- Staff sign the school's Acceptable Use Policy and this includes a clause on the use of mobile phones/personal equipment for taking pictures of pupils;
- If specific pupil photos (not group photos) are used on the school website, in the prospectus or in other high profile publications, the school will obtain individual parental or pupil permission for its long term use;
- Pupils are taught about how images can be manipulated in their e-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 ICT 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 identify 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.

Any equipment that stores data will be disposed of by a GDPR accredited contactor, in accordance with the May guidance.