FLIXTON PRIMARY SCHOOL

ONLINE SAFETY

POLICY

Revised: March 2017
Review: March 2019

Flixton Primary School
Online Policy

Contents

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 Flixton Primary School with respect to the use of ICT-based technologies;
- safeguard and protect the children and staff of Flixton Primary 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's 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
- 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 nude selfies or 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 the Flixton Primary 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 Flixton Primary 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 sites and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other online 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. 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 online 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 • 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 online safety roles and to train other colleagues, as relevant • To be aware of procedures to be followed in the event of a serious online safety incident. • To receive regular monitoring reports from the ISP • 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 Safeguarding Lead	• To take day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school's online safety policies / documents
	• To promote an awareness and commitment to e-safeguarding throughout the school community
	• To ensure that online safety education is embedded across the curriculum
	• To liaise with school's ICT technical staff
	• To communicate regularly with SLT and the designated 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 an online safety incident log is kept up to date
	• facilitates training and advice for all staff
	• To liaise with the Local Authority and relevant agencies
	• To be 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 / Safeguarding Governor	• 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

Role	Key Responsibilities
	the policy. This will be carried out by the Safeguarding Governor 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 • The role of the Safeguarding Governor will include: • regular review with the DSL (including online safety incident logs, filtering / change control logs)
Computing Subject Leader	• To oversee the delivery of the online safety element of the Computing curriculum • To liaise with the DSL regularly
Network Manager/technician (Infant Site)	• To report any online safety related issues that arises, to the DSL • 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's ICT systems • To ensure that access controls / encryption exist to protect personal and sensitive information held on school-owned devices • To ensure the school's procedures for web filtering are applied and updated on a regular basis • To inform Trafford of issues relating to the filtering applied by the LA • To keep up to date with the school's online safety policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant • To monitor the use of the network / remote access / email in order that any misuse / attempted misuse can be reported to the DSL /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
Data Manager	• To ensure that all data held on pupils on the school's office machines have appropriate access controls in place
Teachers	• To embed online safety issues in all aspects of the curriculum and other 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 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 online safety

Role	Key Responsibilities
	coordinator • To maintain an awareness of current online safety issues and guidance e.g. through CPD • To model safe, responsible and professional behaviours in their own use of technology • 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	• 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 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 access the school website / on-line student / pupil records in accordance with the relevant school Acceptable Use Agreement. • 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 and wider school community in the following ways:

- Policy to be posted on the school's websites/ staffrooms/ classrooms
- Policy to be part of school's induction pack for new staff
- Acceptable use agreements discussed with staff at the start of each year.
- Acceptable use agreements to be held in personnel files

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:
    - Sanctions available under the school's discipline policy.
    - 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];
    - referral to LA / Police.

- Our DSL 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's Safeguarding Policy.

Review and Monitoring

- The school has a DSL who will be responsible for document ownership, review and updates.
- The online safety policy will be reviewed bi-annually or when any significant changes occur with regard to the technologies in use within the school
- All amendments to the school's online safeguarding policy will be discussed in detail with all members of teaching staff.

2. Education and Curriculum

Pupil online safety curriculum

The school has

- A clear, progressive online safety education programme as part of the Computing curriculum / PSHE curriculum. It is built on national guidance. This covers a range of skills and behaviours appropriate to their age and experience, including:
    - the use and dissemination of SMART rules;
    - 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;
    - 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;
    - 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, Digi-tell via the school's websites, or an organisation such as ChildLine or the CLICK CEOP button.

- Planned Internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.
- Ensured staff will model safe and responsible behaviour in their own use of technology during lessons.
- Ensured 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;
- Ensured 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

Our 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 online safety issues and the school's online safety education programs;
- 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

Our school

- Has advice, guidance and training available for parents, including:
    - Information leaflets; in school newsletters; on the school web site;
    - suggestions for safe Internet use at home;
    - provision of information about national support sites for parents.

3. Incident Management

In our 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 contributes to developments in policy and practice in online safety within the school. The records are reported to the school's senior leaders and Governors
- 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**

Our school:

- Has educational filtered secure broadband connectivity through Trafford (Infant site) and MGL (Junior site)
- Ensures network health through use of anti-virus software and network set-up so staff and pupils cannot download executable files;
- Uses DfE or LA approved systems such as S2S, secured email to send personal data over the Internet and use encrypted devices or secure remote access 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;

- Are vigilant in their supervision of pupils' use at all times, as far as is reasonable, and use common-sense strategies in learning resource areas where older pupils have more flexible access;
- Ensure all staff have signed an acceptable use agreement form and understand that they must report any concerns;
- Are vigilant when conducting 'raw' image search with pupils e.g. Google image search;
- Inform all users that Internet use is monitored;
- Inform staff and students that that they must report any failure of the filtering systems directly to the *teacher*. Our system administrator logs or escalates as appropriate to the Technical service provider or Trafford Helpdesk as necessary;
- Make 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;
- Provide advice and information on reporting offensive materials, abuse/ bullying etc. available for pupils, staff and parents
- Immediately refer any material we suspect is illegal to the appropriate authorities – Police – and the LA.

- **Network management (user access, backup)**
  Our school
  - 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 services and policies
  - Ensures storage of all data within the school will conform to the UK data protection requirements
  - Ensures 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.

To ensure the network is used safely, our 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.
- Ensures staff access to the school's management information system is controlled through a separate password for data security purposes;
- Makes clear that no one should log on as another user;
- Requires all users to always log off when they have finished working or are leaving the computer unattended;
- Requires users, where they find a logged-on machine, to always log-off and then log-on again as themselves.
- Has set-up the network so that users cannot download executable files / programmes;

- Have blocked access to music/media download or shopping sites – except those approved for educational purposes;
- Scan all mobile equipment with anti-virus / spyware before it is connected to the network;
- Make 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;
- Make 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.
- Make 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.
- Maintain 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
- Have 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;
- Ensure that access to the school's network resources from remote locations by staff is restricted and access is only through school / LA approved systems:
- Do 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 MIS Support
- Make clear responsibilities for the daily back up of MIS and finance systems and other important files;
- Have a clear disaster recovery system in place for critical data that includes a secure, remote back up of critical data, that complies with external Audit's requirements;
- Use the DfE secure s2s website for all CTF files sent to other schools;
- Follow ISP advice on Local Area and Wide Area security matters and firewalls and routers have been configured to prevent unauthorised use of our network;
- Secures our wireless networks to appropriate standards suitable for educational use;
- Review the school ICT systems regularly with regard to health and safety and security.

Password policy

- Flixton Primary 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's systems. Staff are responsible for keeping their password private.

E-mail

Our school

- Provides staff with an email account for their professional use and makes clear personal email should be through a separate account;
- Does not publish personal e-mail addresses of pupils or staff on the school website.
- 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 e mails dangerous.

Pupils:

- Pupils are introduced to, and use e-mail as part of the ICT/Computing scheme of work.
- Pupils are taught about the safety and 'netiquette' of using e-mail both in school and at home i.e. they are taught:
    - not to give out their e-mail 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 e-mail is a form of publishing where the message should be clear, short and concise;
    - that any e-mail 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 e-mail, 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 if they receive an e-mail 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 e-mails, but to keep them as evidence of bullying;
    - not to arrange to meet anyone they meet through e-mail without having discussed with an adult and taking a responsible adult with them;

- that forwarding 'chain' e-mail letters is not permitted.

Staff:

- Access in school to external personal e mail accounts may be blocked
- Never use open email to transfer staff or pupil personal data. We use secure, LA / DfE approved systems. These include: S2S (for school to school transfer) or encrypted school email.
- Staff know that confidential information in emails are to be sent from the headteacher's or the office secure email accounts.
- 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 AUP to say they have read and understood the online safety rules, including e-mail and we explain how any inappropriate use will be dealt with.

School's websites

- The Headteacher takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained;
- The school's websites comply with the statutory DfE guidelines for publications;
- The point of contact on the websites is the school address, telephone number and we use a general email contact address, e.g. flixtoninfants.admin@trafford.gov.uk or admin@flixtonjuniorschool.couk
- Home information or individual e-mail identities 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

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 school's preferred system for such communications.

- The school's preferred system for social networking will be maintained in adherence with the communications policy.

School's 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.

Technical Solutions

- Staff have encrypted portable drives to store sensitive documents or photographs.
- We require staff to log-out of systems when leaving their computer
- We use encrypted flash drives if any member of staff has to take any sensitive information off site.
- We use the DfE S2S site to securely transfer CTF pupil data files to other schools.
- We lock any back-up tapes in a secure, fire-proof cabinet. No back-up tapes leave the site on mobile devices.
- 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 that once contained personal data.
- Portable equipment 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.

6. Equipment and Digital Content

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 hand held device brought into the school.
- If children bring mobile phones into our school, they must switch them off and take them to the relevant school office at the start of the day. The phones will be returned to them at the end of the day. Any phones found in school during the school day will be confiscated and only returned to a parent.
- Staff members may use their phones during school break times in staff only areas. All visitors are requested to keep their phones on silent.
- The recording, taking and sharing of images, video and audio on any mobile phone is prohibited; 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's 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.
- Staff may use their phones during break times. If a staff member is expecting a personal call they may leave their phone with the relevant 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 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 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. 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.
- 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.

Staff use of personal devices

- 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 be issued with a school phone where contact with students, parents or carers is required.
- Mobile Phones and personally-owned devices will be switched off or switched to 'silent' mode. Bluetooth communication should be 'hidden' or switched off and mobile phones or personally-owned devices will not be used during teaching periods unless permission has been granted by a member of the senior leadership team in emergency circumstances.
- 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 must 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.
- If a member of staff breaches the school's policy then disciplinary action may be taken.

Digital images and video
In our 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's website, in the prospectus or in other high profile publications the school will obtain individual parental or pupil permission for its long term use
- The school blocks/filters access to social networking sites 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 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.
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.