E-SAFETY POLICY

	Date	Minute No.	Review date
Approved by Governors	01/06/15	1/6/15.14.6	July 2017
V2 Reviewed by Governors	04/07/17	04/07/17.18	July 2019
Reviewed by Governors			

Contents

1. Introduction and overview
   - Rationale and Scope
   - Roles and responsibilities
   - How the policy be communicated to staff/pupils/community
   - Handling complaints
   - Review and Monitoring

2. Education and Curriculum
   - Pupil e-safety Curriculum
   - Staff and governor training
   - Parent awareness and training

3. Expected Conduct and Incident management

4. Managing the ICT infrastructure
   - Internet access, security (virus protection) and filtering
   - Network management (user access, backup, curriculum and admin)
   - Passwords policy
   - E-mail
   - School website
   - Learning platform
   - Social networking
   - Video Conferencing

5. Data security
   - Management Information System access
   - Data transfer

6. Equipment and Digital Content
   - Personal mobile phones and devices
   - Digital images and video
   - Asset disposal

Appendices:
1. Acceptable Use Agreement (Staff)
2. Acceptable Use Agreement (Pupils)
3. Acceptable Use Agreement including photo/video permission (Parents)
4. Protocol for responding to e-safety incidents
5. Protocol for Data Security
6. Search and Confiscation guidance from DfE

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 Ashover Primary with respect to the use of ICT-based technologies.
- Safeguard and protect the children and staff of Ashover 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 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 cyber bullying 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.

- 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

This policy applies to all members of Ashover Primary 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 Ashover Primary.

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 academy, 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 e-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. - 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.
e-Safety Co-ordinator / 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 technical staff. - To communicate regularly with SLT and the designated Computing 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 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 - cyber-bullying and use of social media
Governors / Computing and E-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 Curriculum Sub Committee receiving regular information about e-safety incidents and monitoring reports. A member of the Governing Body has taken on the role of Computing/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 Co-ordinato

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 Computing/e-Safety coordinator. • 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 Computing 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. • 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. • To ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster.
LEARNING PLATFORM Leader	• 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. • 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 e-Safety policies and guidance. • To read, understand, sign and adhere to the school staff Acceptable Use 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. • 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.

Role	Key Responsibilities
Pupils	• Read, understand, sign and adhere to the Pupil Acceptable Use Policy (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 cyber-bullying. • 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 / on-line 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.

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

- Policy to be posted on the school website.
- 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 with Computing/ e-Safety Coordinator / Headteacher;
    - informing parents or carers;
    - removal of Internet or computer access for a period,
    - 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 cyber bullying 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: Computing policy, Child Protection policy, Anti-Bullying policy, Behaviour policy, Personal, Social and Health Education and for Citizenship policies.

- The school has an e-safety coordinator who will be responsible for document ownership, review and updates.

- The e-safety policy will be reviewed annually 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 Computing/e-safety 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. 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 / PSHE curriculum. It is built on SWGfL e-Safeguarding and e-literacy framewok for EYFS to Y6 and national guidance. 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;
    - 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;

- o 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;
- o 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;
- o to understand why they must not post pictures or videos of others without their permission;
- o to know not to download any files – such as music files - without permission;
- o to have strategies for dealing with receipt of inappropriate materials;
- o [for older pupils] to understand why and how some people will 'groom' young people for sexual reasons;
- o to understand the impact of cyber bullying, sexting and trolling and know how to seek help if they are affected by any form of online bullying;
- o to know how to report any abuse including cyber bullying; 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.
- 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.
- 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;
- 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 with information and guidance on the eSafeguarding 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 on internet safety awareness day in February.
- Holds training events for parents to raise the profile of e-safety.

3. Expected Conduct and Incident management

Expected conduct
In school all users:
- o 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.);

- o need to understand the importance of misuse or access to inappropriate materials and are aware of the consequences;
- o need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so;
- o 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;
- o 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
- o 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.

Pupils
- o Should have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.

Parents/Carers
- o 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.
- o Should know and understand what the 'rules of appropriate use' are and what sanctions result from misuse.

Incident Management
In school:
- o 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;
- o 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;
- o support is actively sought from other agencies as needed (eg the local authority and regional broadband grid, UK Safer Internet Centre helpline) in dealing with e-safety issues;
- o monitoring and reporting of e safety incidents takes place and contribute to developments in policy and practice in e-safety within the school;
- o parents / carers are specifically informed of e-safety incidents involving young people for whom they are responsible;
- o 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:
- o Has educational filtered secure broadband connectivity.

- o Uses the Mercurycloud web filtering system. The Mercurycloud web filter uses the Websense master database for URL categorisation with more than 60 million websites in more than 95 categories. Sites are then inspected and blocked accordingly based on 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 when permission has been sought.

- o Ensures network remains healthy through use of anti-virus software and network set-up so staff and pupils cannot download executable files.
- o Uses a secured email system to send personal data over the Internet and uses encrypted devices or secure remote access were staff need to access personal level data off-site.
- o Blocks all Chat rooms and social networking sites except those that are part of an educational network or approved Learning Platform.
- o Has blocked pupil access to music download or shopping sites – except those approved for educational purposes
- o Works to ensure any concerns about the system are communicated so that systems remain robust and protect students.
- o 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.
- o Ensures all staff and students have signed an acceptable use agreement form and understands that they must report any concerns.
- o Ensures pupils only publish within an appropriately secure environment: the school's learning environment.
- o Requires staff to preview websites before use.
- o Informs all users that Internet use is monitored.
- o Informs staff and students that that they must report any failure of the filtering systems.
- o Makes clear all users know and understand what the 'rules of appropriate use'.
- o Provides advice and information on reporting offensive materials, abuse/ bullying etc available for pupils, staff and parents.
- o Immediately refers any material we suspect is illegal to the appropriate authorities – Police – and the LA.

To ensure the network is used safely, this school:
- Ensures staff read and sign that they have understood the school's e-safety Policy.
- Provide pupils with an individual network log-in username.
- All pupils have their own unique username and password which gives them access to the Learning Platform.
- 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.
- Requires all staff 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.
- Has blocked access to music/media download or shopping sites – except those approved for educational purposes.
- 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 mainly to support their professional responsibilities and that they notify the school of any "significant personal use" as defined by HM Revenue & Customs.

- 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.

- 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.

- Provides pupils and staff with access to content and resources through the approved Learning Platform which staff and pupils access using their username and password.

- Makes clear responsibilities for the daily back up of MIS and finance systems and other important files.

- Has 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.

- Uses the DfE secure s2s website for all CTF files sent to other schools.

- Ensures that all pupil level data or personal data sent over the Internet is encrypted or only sent within the approved secure system in our LA.

- Follows maintenance company advice on 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.

Passwords 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.

- 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 'STRONG' passwords for access into the MIS system.

- We require staff to change their passwords into the MIS system every 60 days.

E-mail

This school

- Provides staff with an email account for their professional use.

- Does not publish personal e-mail addresses of staff on the school website. We use anonymous or group e-mail addresses, for example enquiries@schoolname.la.sch.uk / headteacher@schoolname.la.sch.uk 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 e mails dangerous.

Pupils:
- Pupils are introduced to, and use e-mail as part of the Computing scheme of work.
- Year R/1 pupils are introduced to principles of e-mail.
- 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;
  - 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.

- Pupils sign the 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.

Staff:
- Staff can have access to a school e mail address.
- Access in school to external personal e mail accounts may be blocked.
- Never use email to transfer staff or pupil personal data. We use secure, LA / DfE approved systems.
- 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:
  - 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 LA / 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.
  - Uploading of information is restricted to our website authorisers.
  - 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.

- The point of contact on the web site is the school address, telephone number and we use a general email contact address, e.g. enquiries@schooladdress or admin@schooladdress. 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 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' Learning Platform / virtual learning space is shared between different staff members according to their responsibilities e.g. all class teachers upload information in their class areas.

- Photographs and videos uploaded to the schools LEARNING PLATFORM 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 Learning Platform.

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.

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.

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.

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

  - staff,

- o governors,
- o pupils
- o parents

This makes clear staffs' responsibilities with regard to data security, passwords and access.

- We follow LA guidelines for the transfer of any data, such as MIS 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 Protect and Restricted material must be encrypted if the material is to be removed from the school and limit such data removal.

- School staff with access to setting-up usernames and passwords for email, network access and Learning Platform access are working within the approved system and follow the security processes required by those systems.

- We ask staff to undertaken at least annual house-keeping to review, remove and destroy any digital materials and documents which need no longer be stored.

Technical Solutions

- Staff have a secure area on the network 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.

- All servers are stored in lockable locations and are managed by DBS-checked staff.

- The disaster recovery plan details how data is backed up and can be recovered in an emergency.

- We use an approved or recommended disposal company for disposal of equipment where any protected or restricted data has been held.

- Portable equipment loaned by the school (for use by staff at home), where used for any protected data.

6. Equipment and Digital Content

Personal mobile phones and mobile devices
- Designated 'mobile use free' areas are situated in the setting, and signs to this effect are to be displayed throughout. The areas which should be considered most vulnerable include: toilets, bathrooms and in some settings - sleep areas and changing areas.

- Mobile phones brought into school are entirely at the staff member, pupil'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 school.

- Student mobile phones which are brought into school must be turned off (not placed on silent) and stored in the school office on arrival at school. They must remain there until the end of the day. Staff members may use their phones during school break times. 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 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 pupils 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 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. 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 teacher.

- 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.

- All mobile phones and personally-owned devices will be handed in at the office should they be brought into school.

Pupils' use of personal devices

- The School strongly advises that pupil 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.

- If a pupil 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. Pupils found in possession of a mobile phone during an exam will be reported to the appropriate examining body.

- If a pupil needs to contact his or her parents or carers in specific situations, 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.

- Pupils should protect their phone numbers by only giving them to trusted friends and family members. Pupils will be instructed in safe and appropriate use of mobile phones and personally-owned devices and will be made aware of boundaries and consequences.

- No students should bring his or her mobile phone or personally-owned device into school. Any device brought into school will be confiscated.

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 permitted in the case of trips and residentials where contact with parents or carers may be 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.
- If a member of staff breaches the school policy then disciplinary action may be taken.

Digital images and video
In this school:

- We gain parental / carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter / son joins the school.
- 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 web site, in the prospectus or in other high profile publications the school will obtain individual parental or pupil permission for its long term use.
- The school blocks/filter 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 eSafety 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.

Written March 2015
Reviewed June 2016