Future Schools Trust

E-Safety Policy

June 2016

Contents

1. Introduction and Overview

Rationale

The purpose of this policy is to:

- Set out the key principles expected of all members of Future Schools Trust with respect to the use of ICT-based technologies.
- Safeguard and protect the pupils and staff of Future Schools Trust.
- Assist Trust staff working with pupils 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 Trust policies.
- Ensure that all members of the Trust 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 pupils.

The main areas of risk for our Trust 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 including all characteristics considered protected under the equality act.
- 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 Future Schools Trust community (including staff, pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of Trust/ Academy ICT systems, both in and out of Future Schools Trust.

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 *Trust/Academy* site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

The *Trust/Academy* 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 Trust.

Role	Key Responsibilities
Headteachers Cornwallis New Line Learning Tiger	• To take overall responsibility for e-safety provision • To take overall responsibility for data and data security • To ensure the Trust 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 Co-ordinator / 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)
E-Safety Co-ordinator & Designated Safeguarding Lead DSL – NLL DSL – Cornwallis E-Safety Co-ordinator	• takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the Trust e-safety policies / documents • promotes an awareness and commitment to e-safeguarding throughout the Trust community • ensures that e-safety education is embedded across the curriculum • liaises with Trust 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 - cyber-bullying and use of social media
Governors/E-safety governor	• To ensure that the Trust follows all current e-safety advice to keep the pupils 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 Trust in encouraging parents and the wider community to become engaged in e-safety activities • The role of the E-Safety Governor will include:

Role	Key Responsibilities
	• regular review with the E-Safety Co-ordinator (including e-safety incident logs, filtering/change control logs).
Network Manager/ICT technicians	• To report any e-safety related issues that arises, to the e-safety coordinator. • To ensure that users may only access the Trust'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 Trust ICT system • To ensure that access controls / encryption exist to protect personal and sensitive information held on Trust-owned devices • the Trust's policy on web filtering is applied and updated on a regular basis • that he/she keeps up to date with the Trust'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/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 Trust's e-security and technical procedures
Data Team	• To ensure that all data held on pupils on the Trust office machines have appropriate access controls in place.
Teachers	• To embed e-safety issues in all aspects of the curriculum and other Trust activities • To supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extra-curricular and extended Trust 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 • To report any suspected misuse or problem to the e-safety coordinator • Teachers will have E-Safety training annually included within the safeguarding. • Staff must abide by the staff code of conduct
All staff	• To read, understand and help promote the Trust's e-safety policies and guidance • 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 Trust policies with regard to these devices • To report any suspected misuse or problem to the e-safety co-ordinator • 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 must be on a professional level and only through Trust based systems, never through personal mechanisms, e.g. email, text, mobile phones etc. • All staff will have E-Safety training annually included within the safeguarding.

Role	Key Responsibilities
Pupils	• Read, understand, sign and adhere to the Pupil E-Safety Policy agreement • 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 Trust policy on the use of mobile phones, digital cameras and hand held devices. • To know and understand Trust 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 Trust and realise that the Trust's E-Safety Policy covers their actions out of Trust, if related to their membership of the Trust • To take responsibility for learning about the benefits and risks of using the Internet and other technologies safely both in Trust and at home • To report any suspected misuse or problem to the e-safety co-ordinator
Family Officer	• Educating Parents and raising awareness as instructed by DSL and E-Safety coordinator. • Information on the website for parents.
Parents/ guardians	• To read, understand and promote the Trust E-Safety Policy with their children and sign the Agreement. • To access the Trust's website/VLE/SLG/pupil records in accordance with the relevant Trust E-Safety Policy. • To consult with the Trust if they have any concerns about their children's use of technology.
External groups	• Some external individuals/organisation (orange lanyard) may need access to equipment/system internet access but will sign an Acceptable Use Policy. Visitors on a red lanyard will not be issued with any access to our systems.

Communication:

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

- Policy to be posted on the Trust website/Access/ issued to new starters.
- Policy to be part of Trust induction pack for new staff.
- E-Safety Policy agreements discussed with pupils at the start of each year.
- E-Safety Policy agreements to be issued to whole Trust community, usually on entry to the Trust.
- E-Safety Policy agreements to be held in pupil and HR files.

Handling complaints:

- The Trust 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 Trust computer or mobile device. Neither the Trust 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 Year/E-Safety Co-ordinator/ 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];
  - referral to LA/Police.

- Our E-Safety Co-ordinator / Designated Safeguarding Lead 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, Behaviour and Safeguarding Policy. Complaints related to child protection are dealt with in accordance with Trust / LA child protection procedures.

Review and Monitoring

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

- The Trust has an e-safety coordinator Charles Ealham 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 Trust.
- The e-safety policy has been written by the Trust e-safety Coordinator and Designated Safeguarding Lead 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 Trust e-safeguarding policy will be discussed in detail with all members of teaching staff.

Version Control

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

Title	Future Trusts Trust E-Safety Policy		
Version	1.3		
Date	19/03/2015		
Author	E-safety Co-ordinator		
Approved by Headteacher	June 2016		
Approved by Governing Body	June 2016		
Next Review Date	01/03/2017		
Modification History			
Version	Date	Description	Revision Author
1.0	05/02/2015	Initial draft	E-safety Co-ordinator
1.2	05/03/2015	Version 1.2	E-safety Co-ordinator
1.3	19/03/16	Version 1.3	E-safety Co-ordinator
1.4	09/06/16	Version 1.4	E-safety Co-ordinator

2. Education and Curriculum

Pupil e-safety curriculum

This Trust/Academy

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

- Plans Internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.
- Will remind pupils about their responsibilities through an end-user Policy which every pupil will sign/will be displayed throughout the Trust/will be displayed when a pupil logs on to the Trust 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

The Trust

- 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 Trust's e-safety education program; annual updates.
- 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-safety policy.

3. Expected Conduct and Incident management

Expected conduct

In the Trust all users:

- Are responsible for using the Trust ICT systems in accordance with the relevant E-Safety Policy agreement which they will be expected to sign before being given access to Trust 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 Trust and realise that the Trust's E-Safety Policy covers their actions out of Trust, if related to their membership of the Trust
- Will be expected to know and understand Trust policies on the use of mobile phones. They should also know and understand Trust policies on the taking / use of images and on cyber-bullying

Staff

- Are responsible for reading the Trust's e-safety policy, acceptable use policy, online social networking policy and using the Trust's ICT systems accordingly.
  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 Policy agreement form at time of their child's entry to the Trust.

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

Incident Management

In this Trust/Academy:

- 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 Trust'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 Trust. The records are reviewed/audited and reported to the Trust's senior leaders, Governors /the LA where appropriate.
- 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
- Each site within the Trust will hold an E-Safety breach folder where it records data of the incident and outcome.

4. Managing the ICT infrastructure

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

The Trust:

- Has the educational filtered secure broadband connectivity through the Trusts Broadband Service.
- Uses the SBS Lightspeed filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature, etc. All changes to the filtering policy is logged and only available to staff with the approved 'web filtering management' status;
- Uses user-level filtering where relevant, thereby closing down or opening up options appropriate to the age / stage of the pupils;
- Ensures the network remains healthy through use of McAfee anti-virus software etc. and network set-up so staff and pupils cannot download executable files;
- Blocks all Chat rooms 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 pupil access to music download or shopping sites – except those approved for educational purposes at a regional or national level, such as Audio Network;
- Uses network security time-outs on Internet access where practicable / useful;

- 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 pupils have signed an e-safety policy agreement form and understands that they must report any concerns;
- Ensures pupils only publish within an appropriately secure environment : the Trust's virtual learning environment or other secure platforms etc.
- Requires staff to preview websites before use [where not previously viewed or cached] and encourages use of the Trust's virtual Learning Platform as a key way to direct pupils to age / subject appropriate web sites; 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 Safe Search.
- Never allows / Is vigilant when conducting 'raw' image search with pupils e.g. Google image search;
- Informs all users that Internet use is monitored;
- Informs staff and pupils that that they must report any failure of the filtering systems directly to the Network Manager. Our system administrator(s) logs or escalates as appropriate to the Technical service provider.
- 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)

The Trust

- Uses individual, audited log-ins for all users
- 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 Trusts Broadband services and policies.
- Storage of all data within the Trust 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.

To ensure the network is used safely, this Trust:

- Ensures staff read and sign that they have understood the Trust'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.
- Laptops/Trust mobile phones or anything with pupil data on if taken home by staff overnight should not be left in cars.
- Staff access to the Trust's management information system is controlled through a separate password for data security purposes.
- We provide pupils with an individual network log-in username. From Year 7 they are also expected to use a personal password.
- Makes clear that no one should log on as another user and makes clear that pupils should never be allowed to log-on or use teacher and staff logins as these have far less security restrictions and inappropriate use could damage files or the network.

- Has set-up the network with a shared work area for pupils and one for staff. Staff and pupils are shown how to save work and access work from these areas.
- Requires all users to always log off 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 Trust 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 Trust, is used solely to support their professional responsibilities and that they notify the Trust 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 ICT Team; equipment installed and checked by approved Suppliers/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 Trust's network resources from remote locations by staff is restricted and access is only through Trust / LA approved systems: *e.g. teachers access their area / a staff shared area for planning documentation via a VPN solution.*
- Does not allow any outside Agencies to access our network remotely except where there is a clear professional need and then access is restricted and is only through approved systems; e.g. technical support or MIS Support, our Education Welfare Officers accessing attendance data on specific children, parents using a secure portal to access information on their child.
- 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 (their network 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 Trusts.
- Ensures that all pupil level data or personal data sent over the Internet is encrypted or only sent within the approved secure system in our LA.
- Follows ISP advice on Local Area and Wide Area security matters and firewalls and routers have been configured to prevent unauthorised use of our network.
- Our wireless network has been secured to industry standard Enterprise security level /appropriate standards suitable for educational use.
- All computer equipment is installed professionally and meets health and safety standards.
- Projectors are maintained so that the quality of presentation remains high.
- Reviews the Trust ICT systems regularly with regard to health and safety and security.

Password policy

- This Trust 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 Trust systems. Staff are responsible for keeping their password private.
- All staff and pupils are required to have a strong password for their e-mail account, this will need to have a capital letter and a number.

E-mail

The Trust

- Provides staff with an email account for their professional use, Future Schools Trust makes clear personal email should be through a separate account;
- Does not publish personal e-mail addresses of pupils on the Trust 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.

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 Trust and at home i.e. they are taught:
  - not to give out their e-mail address unless it is part of a Trust 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 Trust 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.

- Pupils sign the Trust Acceptable Use Policy 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 only use the Trust e-mail systems for professional purposes.

- Access in Trust 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. These include: S2S (for Trust to Trust transfer).
- 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 Trust headed paper. That it should follow the Trust '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 Online Social Networking Policy 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.

Trust 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: (Marketing and Communications Manager).
- The Trust web site complies with the statutory DfE guidelines for publications.
- Most material is the Trust'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 Trust address, telephone number and we use a general email contact address, e.g. office@futureschoolstrust.com individual email addresses are used too.
- We do not use pupils' names when saving images in the file names or in the tags when publishing to the Trust website.
- We do not use embedded geodata in respect of stored images.
- We expect teachers using' Trust approved blogs or wikis to password protect them and run from the Trust website.

Learning platform (VLE)

- Uploading of information on the Trusts' Virtual Learning Environment 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 Trusts Virtual Learning Environment will only be accessible by members of the Trust community.
- In Trust, pupils are only able to upload and publish within Trust approved and closed systems, such as the Virtual Learning Environment.

Social networking

- Staff are instructed not to run social network spaces for pupil use on a personal basis or to open up their own spaces to their pupils, but to use the Trusts' preferred system for such communications.
- Trust staff will ensure that in private use:
    - No reference should be made in social media to pupils, parents / carers or Trust staff
    - They do not engage in online discussion on personal matters relating to members of the Trust community

- Personal opinions should not be attributed to the *Trust /academy* 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 Trust as part of our site surveillance for staff and pupil 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. CCTV can only be viewed by staff if the Headteacher, SLT or Designated Safeguarding Lead have given authorisation.

5. Data security: Management Information System access and Data transfer

Strategic and operational practices

The Trust

- Staff are clear who are the key contact(s) for key Trust 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 which is kept within the HR Department.

  We ensure ALL the following Trust stakeholders sign an E-Safety Policy agreement form. We have a system so we know who has signed.
    - staff,
    - governors,
    - pupils
    - parents / carers

  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 Trust and limit such data removal. We have an approved remote access solution so staff can access sensitive and other data from home, without need to take data home.
- Trust staff with access to setting-up usernames and passwords for email, network access and Virtual Learning Environment 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

- We require staff to log-out of systems when leaving their computer, but also enforce lock-out after 10 minutes' idle time.
- 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 Trusts.
- We use VPN solution with its 2-factor authentication for remote access into our systems.

- We store any Protect and Restricted written material in lockable storage cabinets in a lockable storage area or office.
- All servers are in lockable locations and managed by DBS-checked staff. These rooms are limited as to which staff have access.
- 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 Trust (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 / collected by secure data disposal service.

6. Equipment and Digital Content

Personal mobile phones and mobile devices

- Mobile phones brought into Trust are entirely at the staff member, pupil's & parents' or visitors own risk. The Trust accepts no responsibility for the loss, theft or damage of any phone or hand held device brought into Trust.
- Pupil mobile phones which are brought into Trust must be turned off, placed on silent or kept out of sight. Pupils are allowed to use their phones during break/lunch times.
- 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 site DSL and Marketing and Communications Manager. Such authorised use is to be monitored and recorded. All mobile phone use is to be open to scrutiny and the DSL is to be able to withdraw or restrict authorisation for use at any time if it is to be deemed necessary.
- The Trust reserves the right to search the content of any mobile or handheld devices on the Trust 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.
- Mobile phones and personally-owned devices will not be used in any way during lessons or formal Trust time. They should be switched off or silent at all times.
- Mobile phones and personally-owned mobile devices brought in to Trust are the responsibility of the device owner. The Trust 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 Trust site, e.g. changing rooms and toilets.
- Mobile phones will not be used during lessons or formal Trust 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 DSL.

Pupils' use of mobile phones

- The Trust strongly advises that pupil mobile phones should not be brought into Trust.
- The Trust 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 Trust's policy then the phone will be confiscated and will be held in a secure place with the year team or member of staff. Mobile phones will be released to parents or carers in accordance with the Trust policy.
- Phones 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. This may result in the pupil's withdrawal from either that examination or all examinations.
- 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.
- If any pupil (s) take photos on a personal device/mobile phone on a Trust environment then the Trust reserves the right to remove or delete these images.

Staff use of personal devices

- Staff handheld devices, including mobile phones and personal cameras must be noted in Trust – name, make & model, serial number. Any permitted images or files taken in Trust must be downloaded from the device and deleted in Trust before the end of the day.
- Staff are not permitted to use their own mobile phones or devices for contacting children, young people or their families within or outside of the setting in a professional capacity.
- Staff will be issued with a Trust phone where contact with pupils, 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 the DSL or Marketing and Communications Manager 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 DSL or Marketing and Communications Manager.
- Staff should not use personally-owned devices, such as mobile phones or cameras, to take photos or videos of pupils and will only use work-provided equipment for this purpose.
- If a member of staff breaches the Trust's policy then disciplinary action may be taken.
- Where staff members are required to use a mobile phone for Trust duties, for instance in case of emergency during off-site activities, or for contacting pupils or parents, then a Trust mobile phone will be provided and used. In an emergency where a staff member doesn't have access to a Trust-owned device, they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes.

Digital images and video

In this Trust:

- We gain parental/carer permission for use of digital photographs or video involving their child as part of the Trust agreement form when their daughter/son joins the Trust;
- We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published Trust produced video materials / DVDs.
- Staff sign the Trust'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 Trust web site, in the prospectus or in other high profile publications the Trust will obtain parental permission from the Image Consent Form.
- The Trust 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 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 Well Being curriculum.
- 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 Trust. 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 Trust-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 Trust 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.