POLICY:	**Online Safety**
STATUS:	**Statutory (Safeguarding)**
REVIEWED BY:	**TEFAT 2015**
Date of next Review:	**September 2017**

The Legal Framework

The Education and Inspections Act 2006 empowers Principals / Principals to such extent as is reasonable, to regulate the behaviour of pupils when they are off the academy site 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 academy, but is linked to membership of the academy.

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 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 online behaviour that take place outside academy.

This policy applies to all members of the Elliot Foundation community (including staff, pupils / pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of academy ICT systems, both in and out of <academy name>.

The policy is on two parts – Part A is an overarching policy for the Elliot Foundation and applies to all academies. It should be adapted with individual academy names. Part B provides a template for academies to adapt to the detail of their own specific circumstances.

Part A Overarching Policy

Introduction and Overview

Rationale

The purpose of this policy is to:

- safeguard and protect the children and staff of <Name of academy>.

- set out the key principles expected of all members of the Elliot Foundation community at <Name of academy> with respect to the use of the internet and connected technologies.

- assist academy 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 academy policies.

- ensure that all members of the academy 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 children 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 (lack of care or consideration for intellectual property and ownership – such as music and film)

Key Responsibilities

The Local Governing Body

- Should nominate a specified governor to monitor the effectiveness of online safety. This may be the same individual as the nominated Safeguarding Governor.
- Must ensure that the academy appoints an Online Safety Co-ordinator
- The role of the Online Safety Governor will include regular reviews with the academy’s Online Safety Co-ordinator to consider online safety incident logs, filtering issues and other relevant logs and reports.
- Must identify a method e.g. via reports to a committee to receive regular information about online safety incidents and monitoring reports.
- Must ensure that the academy follows all current online safety advice to keep the children and staff safe
- Must approve the Online Safety Policy and review its effectiveness
- Should support the academy in encouraging parents and the wider community to become engaged in online safety activities.

The Principal

- Must take overall responsibility for online safety provision
- Must take overall responsibility for data and data security
- Will ensure the academy uses an approved, filtered internet service, which complies with current statutory requirements e.g RM Safeclix or similar
- Is responsible for ensuring that staff receive suitable training to carry out their online safety roles and to train other colleagues, as relevant
- Must be aware of procedures to be followed in the event of a serious online safety incident.
- Should receive regular monitoring reports from the Online safety Co-ordinator / Officer
- Is 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)

The Online Safety Co-ordinator / Designated Senior Person (Safeguarding DSP)

- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the academy online safety policies / documents
- promotes an awareness and commitment to online safeguarding throughout the academy community
- ensures that online safety education is embedded across the curriculum
- liaises with academy ICT technical staff
- communicates regularly with SLT and the designated online safety governor / committee to discuss current issues, review incident logs and filtering or other relevant documents and logs
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident
- ensures that an online safety incident log is kept up to date
- facilitates training and advice for all staff
- liaises with the Elliot Foundation and relevant agencies (including the local authority if relevant)
- maintains up to date professional knowledge about online safety issues and legislation, and is 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

The Computing Curriculum Leader

- oversees the online safety element of the computing curriculum
- liaises with the online safety coordinator regularly

Network Manager / Technical Support

- must report any online safety related issues that arise to the online safety coordinator,
- must ensure that users may only access the academy's networks through an authorised and properly enforced password protection policy, in which passwords are regularly changed
- must ensure that provision exists for misuse detection and malicious attack e.g. keeping virus protection up to date
- must ensure the security of the academy ICT system
- must ensure that access controls / encryption exist to protect personal and sensitive information held on academy-owned devices through
  - ensuring that the academy's policy on web filtering is applied and updated on a regular basis
  - keeping up to date with the academy's online safety policy and technical information in order to effectively carry out her / his online safety role and to inform and update others as relevant
  - that the use of the network or any Virtual Learning Environment / remote access / email is regularly monitored in order that any
- 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 academy's e-security and technical procedures
- Must ensure that all data held on pupils on the academy office machines have appropriate access controls in place

Teachers & Teaching Assistants

are expected:

- To embed online safety issues in all aspects of the curriculum and other academy 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
- To read, understand and help promote the academy's online safety policies and guidance
- To read, understand, sign and adhere to the academy 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 academy policies with regard to these devices
- To report any suspected misuse or problem to the online safety coordinator
- To maintain an awareness of current online 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 academy based systems, never through personal mechanisms, e.g. email, text, mobile phones etc.

Pupils

are expected to:

- read, understand, sign and adhere to the Pupil Acceptable Use Policy (NB: at KS1 it would be expected that parents / carers would sign on behalf of the pupils)
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- to understand the importance of reporting abuse, misuse or access to inappropriate materials
- know what action to take if they or someone they know feels worried or vulnerable when online
- know and understand academy policy on the use of mobile phones, digital cameras and hand held devices
- know and understand academy policy on the taking / use of images and on cyber-bullying.
- understand the importance of adopting good online safety practice when using digital technologies out of academy and realise that the academy's Online Safety Policy covers their actions out of academy, if related to their membership of the academy
- take responsibility for learning about the benefits and risks of using the Internet and other technologies safely both in academy and at home
- help the academy in the creation/ review of online safety policies

Parents

- Are expected to support the academy in promoting online safety and endorse the Parents' Acceptable Use Agreement which includes the pupils' use of the internet and the academy's use of photographic and video images
- Are expected to read, understand and promote the academy Pupil Acceptable Use Agreement with their children

- Are expected to access the academy website and any online pupil records in accordance with the relevant academy Acceptable Use Agreement.
- Are asked to consult with the academy if they have any concerns about their children's use of technology

Communication

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

- Policy to be posted on the academy website/staffroom/ classrooms
- Policy to be part of academy 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 academy community, usually on entry to the academy
- Acceptable use agreements to be held in pupil and personnel files

Handling complaints

The academy Online Safety Coordinator will act as first point of contact for any complaint related to pupils' online behaviour or accessing of inappropriate material. Any complaint about staff misuse must be referred to the Principal. Should the matter not be resolved, complainants may refer to the academy Complaints Policy.

Any complaints of cyberbullying will be dealt with in accordance with the individual academy's Anti-Bullying Policy. Complaints related to child protection will be dealt with in accordance with the individual academy's Safeguarding & Child Protection procedures.

The academy will take all reasonable precautions, as outlined in this policy, to ensure online safety. However, owing to the international scale and connected nature of internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee 100% that unsuitable material will never appear on an academy computer or mobile device supplied by the Elliot Foundation. Neither the academy nor the Trust 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 a teacher, the Online Safety Coordinator or senior member fo staff, including the Principal
- informing parents or carers;
- removal of internet or computer access for a period,
- referral to the police.

Review and Monitoring

The online safety policy should be read alongside other academy and Elliot Foundation policies, including Safeguarding & Child Protection policy, Anti-Bullying policy, Behaviour policy, Personal, Social and Health Education and Citizenship policies .

- Each academy will have an Online Safety Co-ordinator who will be responsible for document ownership, review and academy-specific procedures and updates.
- The Online Safety Policy will be reviewed every two years by The Elliot Foundation or when any significant changes occur with regard to the use of technologies
- The Online Safety Policy will be accompanied by academy-specific procedures written by the individual academy Online Safety Coordinator and is current and appropriate for its intended audience and purpose.
- The policy is agreed by the Local Governing Body and it has been agreed by the SLT and referred to other stakeholders such as the PTA. All updates to this policy will be discussed in detail with all members of teaching staff.

Academy Online Education and Curriculum template policy

Pupil online safety curriculum

This academy

- Has a clear, progressive online safety education programme as part of the Computing curriculum and the PSHE curriculum. It is built on national guidance. This covers a range of skills and behaviours appropriate to children's 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 Acceptable Use Policy which every pupil will sign/will be displayed throughout the academy/will be displayed when a pupil logs on to the academy 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 and gambling.

Staff and governor training

This academy

- 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 academy’s online safety education programme;
- 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 online safety policy and the academy’s Acceptable Use Policies.

Parent awareness and training

- This academy
- Runs a rolling programme of advice, guidance and training for parents, including:
  - introduction of the Acceptable Use Agreements to new parents, to ensure that principles of safe online behaviour are made clear

- information leaflets; in academy newsletters; on the academy web site;
- demonstrations, practical sessions held at academy;
- suggestions for safe Internet use at home;
- provision of information about national support sites for parents.

Expected Conduct and Incident management

Expected conduct

In this academy, all users:

- are responsible for using the academy ICT systems in accordance with the relevant Acceptable Use Policy which they will be expected to sign before being given access to academy 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 online safety practice when using digital technologies out of academy and realise that the academy's Online Safety Policy covers their actions out of academy, if related to their membership of the academy
- will be expected to know and understand academy policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand academy policies on the taking / use of images and on cyber-bullying

Staff

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

Pupils/Pupils

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

Parents/Carers

- should provide consent for pupils to use the Internet, as well as other technologies, as part of the online safety acceptable use agreement form at time of their child's entry to the academy
- should know and understand what the 'rules of appropriate use' are and what sanctions result from misuse

Incident Management

In this academy:

- 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 academy's escalation processes.
- support is actively sought from other agencies as needed (e.g. the local authority and regional broadband grid, UK Safer Internet Centre helpline) in dealing with online safety issues
- monitoring and reporting of online safety incidents takes place and contribute to developments in policy and practice in online safety within the academy. The records are reviewed/audited and reported to the academy's senior leaders and LGB
- 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.

Managing the ICT infrastructure

(Individual academies should use this as a check list with their technical support provider and amend / improve accordingly)

Internet access, security (virus protection) and filtering

This academy:

- Has specialist educational filtered secure broadband connectivity
- Uses a 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 are 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 is healthy through the use of anti-virus software and network set-up so staff and pupils cannot download executable files;
- Uses DfE approved systems to send personal data over the internet
- 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 / digital 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;
- 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 acceptable use agreement form and understands that they must report any concerns;
- Ensures pupils only publish within an appropriately secure environment,
- Requires staff to preview websites before use [where not previously viewed or cached]
- Plans the curriculum context for internet use to match pupils' ability, using child-friendly search engines where more open Internet searching is required; e.g. yahoo for kids or ask for kids , Google Safe Search , …..
- Is vigilant when conducting 'raw' image search with pupils e.g. Google image search;
    - Informs all users that the internet use is monitored;

- Informs staff and pupils that that they must report any failure of the filtering systems directly to a named member of staff
- 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, including the police.

Network management (user access, backup)

This academy

- Uses individual, audited log-ins for all users
- Uses guest accounts occasionally for external or short term visitors for temporary access to appropriate services
- Uses teacher ‘remote’ management control tools for controlling workstations / viewing users / setting-up applications and Internet web sites, where useful;
- Has additional local network auditing software installed;
- Ensures storage of all data within the academy conforms 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 academy:

- Ensures staff read and sign that they have understood the academy’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.
- Staff access to the academy’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 X they are also expected to use a personal password;
- All pupils have their own unique username and password which gives them access to the Internet, the Learning Platform *and (for older pupils) their own academy approved email account*;

- Makes clear that no one should log on as another user and makes clear that pupils should never be allowed to log on or use teacher and staff logins as these have far less security restrictions and inappropriate use could damage files or the network;
- Has set-up the network with a shared work area for pupils and one for staff. Staff and pupils are shown how to save work and access work from these areas;
- Requires all users to always log off 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. [Users needing access to secure data are timed out after XX minutes and have to re-enter their username and password to re-enter the network.];
- 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 and we also automatically switch off all computers at X o'clock to save energy;
- 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 academy 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 academy, is used solely to support their professional responsibilities and that they notify the academy of any "significant personal use" as defined by HM Revenue & Customs.
- Maintains equipment to ensure Health and Safety is followed;
  e.g. projector filters are cleaned; equipment is 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;
- Ensures that access to the academy's network resources from remote locations by staff is restricted and access is only through academy approved systems:

- Does not allow any outside agencies to access our network remotely except where there is a clear professional need and then access is restricted and is only through approved systems; e.g. technical support or the Elliot Foundation;
- 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 our broadband network for our CCTV system and have had set-up by approved partners;
- Uses the DfE secure s2s website for all CTF files sent to other academies;
- 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 or through USO secure file exchange (USO FX);
- 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 academy ICT systems regularly with regard to health and safety and security.

Password policy

- This academy 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 academy systems. Staff are responsible for keeping their password private.
- We require staff to use strong passwords for access into our MIS system and to change them frequently

E-mail

This academy

- Provides staff with an email account for their professional use. Elliot Foundation and our academy policy is that staff personal email should be through a separate personal account.
- Does not publish personal e-mail addresses of pupils or staff on the academy website. We use anonymous or group e-mail addresses, for example head@academyname.co.uk

  - 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. We use a number of technologies to help protect users and systems in the academy, including desktop anti-virus products plus direct email filtering for viruses, trojans, pornography, phishing and inappropriate language.

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

Staff:

- Staff can only use the email systems on the academy system
- Staff only use academy email systems for professional purposes
- Access in the academy to external personal email accounts may be blocked
- Never use email to transfer staff or pupil personal data.*;*
- 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 academy headed paper. That it should follow the academy '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 LA / academy Agreement Form 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.

Academy website

- The Principal 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 academy web site complies with the statutory DfE guidelines for publications;
- Most material is the academy'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 academy address, telephone number and we use a general email contact address, e.g. info@academyaddress or admin@academyaddress. Home information or individual email 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 academy website;
- We do not use embedded geodata in respect of stored images
- We expect teachers using' academy approved blogs or wikis to password protect them and run from the academy website.

Learning platform

- Uploading of information on the academy's 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 academy's Learning Platform only be accessible by members of the academy community;
- Within the academy, pupils are only able to upload and publish within academy approved and closed systems, such as the Learning Platform or in closed Google Groups;

Social networking

- Teachers 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 academy's preferred system for such communications.
- The academy's preferred system for social networking will be maintained in adherence with the communications policy.
- Academy staff will ensure that in private use:
    - No reference should be made in social media to pupils / pupils, parents / carers or academy staff
    - They do not engage in online discussion on personal matters relating to members of the academy community
    - Personal opinions should not be attributed to the *academy /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 academy 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.
- We use specialist lesson recording equipment on occasions as a tool to share best teaching practice. We do not reveal any such recordings outside of the staff and will not use for any other purposes.

Data security: Management Information System access and Data transfer

Strategic and operational practices

At this academy:

- The Head Teacher is the Senior Information Risk Officer (SIRO).
- Staff are clear who are the key contact(s) for key academy information (the Information Asset Owners) are. We have listed the information and information asset owners <in a spreadsheet>.
- 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 single central record
- We ensure that all the following academy stakeholders sign an Acceptable Use Agreement form. We have a system so we know who has signed.
  - staff,
  - governors,
  - pupils
  - parents

  This makes clear staff's responsibilities with regard to data security, passwords and access.
- We follow Elliot Foundation guidelines for the transfer of any data, such as MIS data or reports of children, to other professionals. Where these are working in the Local Authority or their partners in Children's Services / Family Services, Health, Welfare and Social Services, we may use LA systems.
- We require that any Protect and Restricted material must be encrypted if the material is to be removed from the academy 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.
- Academy 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 <secure area(s) on the network to store sensitive documents or photographs>.
- We require staff to log-out of systems when leaving their computer, but also enforce lock-out after <10 minutes idle time>.
- We use the DfE S2S site to securely transfer CTF pupil data files to other academies or schools.
- We store any Protect and Restricted written material in <lockable storage cabinets in a lockable storage area>.
- All servers are <in lockable locations and> managed by DBS-checked staff.
- We <lock any back-up tapes in a secure, fire-proof cabinet>. <Back-ups are encrypted>. <No back-up tapes leave the site on mobile devices.>
- We use < LGfL's GridStore remote secure back-up / named alternative solution> for disaster recovery on our <network / admin, curriculum server(s)>.
- 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 academy (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>.
- <We are using secure file deletion software>.

6. Equipment and Digital Content

INSERT A BULLET POINT HERE ABOUT ACADEMY MOBILE DEVICES INC TABLETS IPADS WHICH IN SOME ACADEMIES ARE OPERATING SEPARATELY FROM THE CORE ACADEMY NETWORK?

Personal mobile phones and mobile devices

- Designated 'mobile use free' areas are situated in the academy, 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 academy are entirely at the staff member, pupils' & parents' or visitors' own risk. The Academy accepts no responsibility for the loss, theft or damage of any phone or hand held device brought into academy.
- Pupil mobile phones which are brought into academy must be turned off (not placed on silent) and stored out of sight on arrival at academy. They must remain turned off and out of sight until the end of the day.
- Staff members may use their phones during academy break times. All staff and 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 Principal. Such authorised use is to be monitored and recorded. All mobile phone use is to be open to scrutiny and the Principal is to be able to withdraw or restrict authorisation for use at any time if it is to be deemed necessary.
- The academy reserves the right to search the content of any mobile or handheld devices on the academy 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 academy day, they should do so only through the academy'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 academy 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 academy time. They should be switched off or silent at all times.
- Mobile phones and personally-owned mobile devices brought in to academy are the responsibility of the device owner. The academy 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 academy site, e.g. changing rooms and toilets.
- Mobile phones will not be used during lessons or formal academy time unless as part of an approved and directed curriculum-based activity with consent from a member of staff.
- The Bluetooth, wifi 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 reception should they be brought into academy.

Pupils' use of personal devices

- The Academy strongly advises that pupil mobile phones should not be brought into academy.
- The Academy 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 academy policy then the phone or device will be confiscated and will be held in a secure place in the academy office. Mobile phones and devices will be released to parents or carers in accordance with the academy policy.
- If a pupil needs to contact his or her parents or carers, they will be allowed to use an academy phone. Parents are advised not to contact their child via their mobile phone during the academy day, but to contact the academy 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.
- Pupils will be provided with academy mobile phones to use in specific learning activities under the supervision of a member of staff. Such mobile phones will be set up so that only those features required for the activity will be enabled.

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 an academy phone where contact with pupils, parents or carers is required.
- Mobile Phones and personally-owned devices must 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.
- If members of staff have an educational reason to allow children to use mobile phones or a personally-owned device as part of an educational activity then it will only take place when approved by the senior leadership team.
- Staff should not use personally-owned devices, such as mobile phones or cameras, to take photos or videos of pupils and will only use work-provided equipment for this purpose.
- If a member of staff breaches the academy policy then disciplinary action may be taken.
- Where staff members are required to use a mobile phone for academy duties, for instance in case of emergency during off-site activities, or for contacting pupils or parents, then an academy mobile phone will be provided and used. In an emergency where a staff member doesn’t have access to a academy-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 academy:

- We gain parental / carer permission for use of digital photographs or video involving their child as part of the academy agreement form when their daughter / son joins the academy;

- We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published academy produced video materials / DVDs;
- Staff sign the academy'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 academy web site, in the prospectus or in other high profile publications the academy will obtain individual parental permission for its long term use
- The academy 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 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 academy. 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 academy-owned hardware will be recorded in a hardware inventory.
- Details of all academy-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 academy 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.

Next Policy Review September 2017