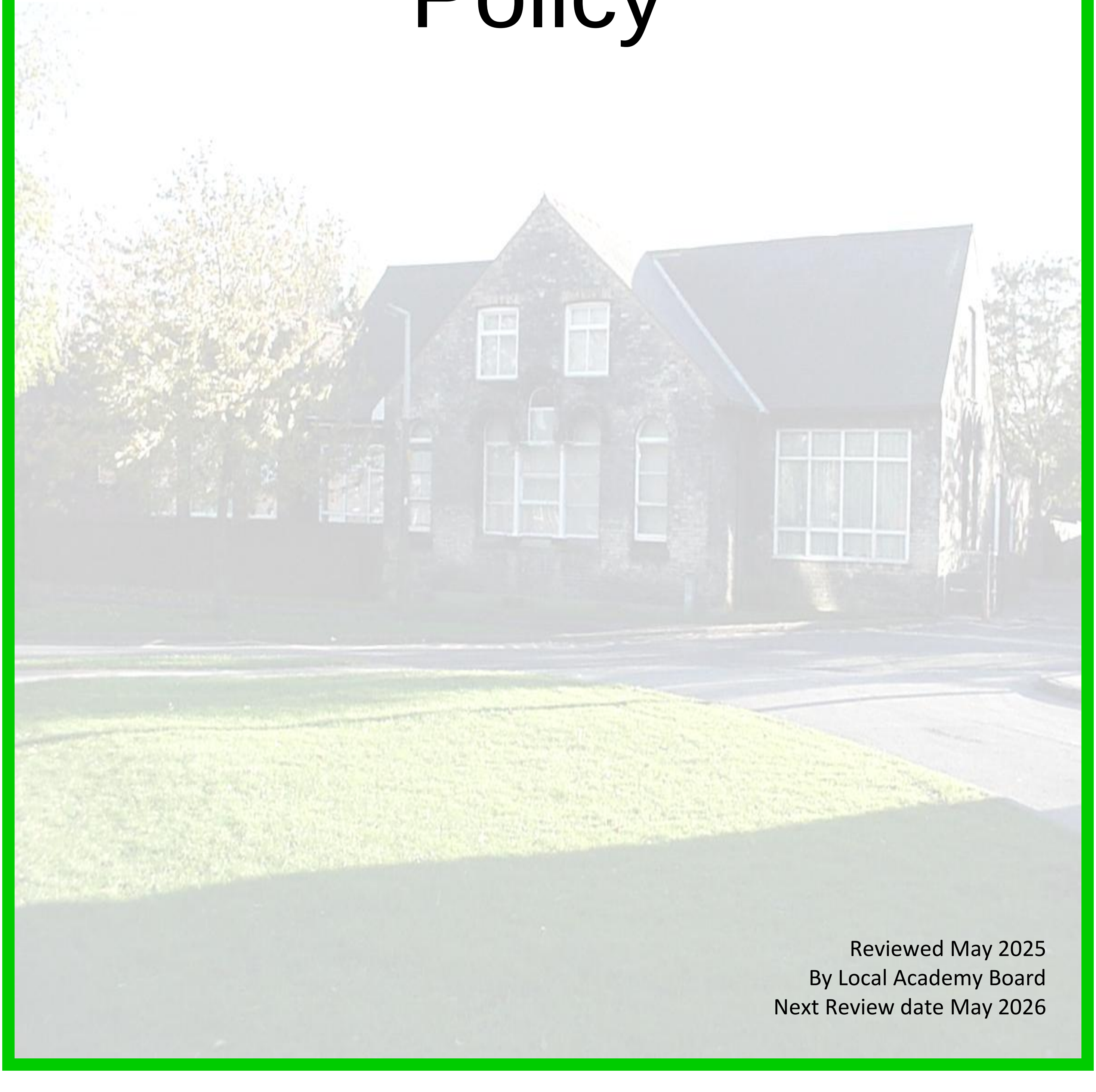
St Botolph's
CE Academy

E-Safety Policy



Reviewed May 2025
By Local Academy Board
Next Review date May 2026

CONTENTS

Appendices

Our Vision

Find your Fantastic
Just as the animals gathered in the safety of the ark, we come together, trusting in God and each other on our journey through life. We persevere, riding the waves through storm and calm, guided by hope, to find our fantastic, no matter what it takes.

1 Introduction

This policy applies to all members of the St Botolph's CE Academy community (including staff, pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of academy digital technology systems, both in and out of the academy.
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 academy site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of online-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 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 safety behaviour that take place out of school.

2 Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within the academy.

Governors

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the *Governors* receiving regular information about online safety incidents and monitoring reports.

Headteacher and Senior Leaders

- The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community
- The Headteacher and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff

Network Manager / Technical staff

The Network Manager / Technical Staff / Headteacher/Executive Head is responsible for ensuring:

- that the academy's technical infrastructure is secure and is not open to misuse or malicious attack

- that the academy meets required online safety technical requirements and any Local Authority / MAT / other relevant body E-Safety Policy / Guidance that may apply
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- the filtering policy is applied and updated on a regular basis
- that they keep up to date with online safety technical information to effectively carry out their online safety role and to inform and update others as relevant
- that the use of the network / internet / Learning Platform / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher for investigation / action / sanction
- that monitoring software / systems are implemented and updated as agreed in academy policies

Teaching and Support Staff

Are responsible for ensuring that:

- they have an up-to-date awareness of online safety matters and of the current academy Online Safety Policy and practices
- they have read, understood and signed the Staff Acceptable Use Agreement
- they report any suspected misuse or problem to the Headteacher/Executive Head for investigation / action / sanction
- all digital communications with pupils / parents / carers should be on a professional level and only carried out using official school systems
- online safety issues are embedded in all aspects of the curriculum and other activities
- pupils understand and follow the E-Safety Policy and acceptable use policies
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Designated Safeguarding Lead

Should be trained in online safety issues and be aware of the potential for serious child protection / safeguarding 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
- online-bullying

Filtering and monitoring

The DSL should also:

- Ensure that the academy has appropriate filters and monitoring systems in place and regularly reviews their effectiveness.
- Monitors network / internet / incident logs with the IT Network Manager
- Receives reports of filtering/online safety incidents and deals with them appropriately
- Review and monitor the school filtering policy and requests for filtering changes in collaboration with the IT Network Manager

Students / Pupils:

- are responsible for using the academy digital technology systems in accordance with the Pupil Acceptable Use Agreement
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on online-bullying.
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the academy's E-Safety Policy covers their actions out of school, if related to their membership of the school

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The academy will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national / local online safety campaigns / literature. Parents and carers will be encouraged to support the academy in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website and on-line pupil records
- their children's personal devices in the academy (where this is allowed)

Any employee found to have violated any aspect of this policy and guidance may be subject to disciplinary action under the academy's Disciplinary Procedure, up to and including termination of employment. All staff will be asked to sign an acceptable Use agreement as part of their induction process – please see **Appendix 1.**

Scope

This policy and guidance applies to both fixed and mobile internet technologies provided by the academy (such as PCs, laptops, personal digital assistants (PDAs), tablets, webcams, whiteboards, voting systems, digital video equipment, etc.) and technologies owned by students and staff, but brought onto academy premises (such as laptops, mobile phones, camera phones, PDAs and portable media players, etc.).

These technologies are to be used for business purposes in serving the interests of our learners and staff in the course of normal operations.

3.E-Safety in the Curriculum

Whilst regulation and technical solutions are very important, their use must be balanced by educating *pupils* to take a responsible approach. The education of *pupils* in online safety /

digital literacy is therefore an essential part of the academy's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities. The curriculum will provide pupils with the correct knowledge and skills to manage the following categories of risk:

- **Content: age-inappropriate or unreliable content can be available to children**
  Some online content is not suitable for children and may be hurtful or harmful. This is true for content accessed and viewed via social networks, online games, blogs and websites. It's important for children to consider the reliability of online material and be aware that it might not be true or written with a bias. Children may need your help as they begin to assess content in this way. There can be legal consequences for using or downloading copyrighted content, without seeking the author's permission.
- **Contact: children can be contacted by bullies or people who groom or seek to abuse them**
  It is important for children to realise that new friends made online may not be who they say they are and that once a friend is added to an online account, you may be sharing your personal information with them. Regularly reviewing friends lists and removing unwanted contacts is a useful step. Privacy settings online may also allow you to customise the information that each friend is able to access. If you have concerns that your child is, or has been, the subject of inappropriate sexual contact or approach by another person, it's vital that you report it to the police via the Child Exploitation and Online Protection Centre (www.ceop.police.uk). If your child is the victim of cyberbullying, this can also be reported online and offline. Reinforce with your child the importance of telling a trusted adult straight away if someone is bullying them or making them feel uncomfortable, or if one of their friends is being bullied online.
- **Conduct: children may be at risk because of their own behaviour, for example, by sharing too much information**
  Children need to be aware of the impact that their online activity can have on both themselves and other people, and the digital footprint that they create on the internet. It's easy to feel anonymous online and it's important that children are aware of who is able to view, and potentially share, the information that they may have posted. When using the internet, it's important to keep personal information safe and not share it with strangers. Discuss with your child the importance of reporting inappropriate conversations, messages, images and behaviours and how this can be done**.**
- **Commerce: young people can be unaware of hidden costs and advertising in apps, games and websites and can be exposed to commercial pressures and scams.**
  Young people's privacy and enjoyment online can sometimes be affected by advertising, in app purchases and marketing schemes, which can also mean inadvertently spending money online, for example within applications. Encourage your children to keep their personal information private, learn how to block both pop ups and spam emails, turn off in-app purchasing on devices where possible, and use a family email address when filling in online forms. They can also be affected by scams, fake competitions and misuse of personal data. Through lessons and guidance, pupils learn to recognise persuasive commercial tactics, avoid financial risks, and seek adult support before making online purchases or entering competitions.

This will be provided in the following ways:

- A planned online safety curriculum is provided as part of Computing / PHSE / other lessons and is regularly revisited
- Pupils are taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.

- Pupils will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils will be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.
- Pupils will be helped to understand the need for the Pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside the academy.
- Staff will act as good role models in their use of digital technologies, the internet and mobile devices
- in lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, staff are vigilant in monitoring the content of the websites the young people visit.

Students with additional needs

St Botolph's Academy endeavours to ensure we create a consistent message with parents of all students. However, staff are aware that some students may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of onlin safety issues.
Where a pupil has additional needs in respect of social understanding, careful consideration should be given to group interactions when raising awareness of E-Safety. Internet activities must be planned and well managed for these children and young people.

Education – Parents / Carers
Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.
The academy will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters, web site
- Parents / carers evenings
- High profile events / campaigns e.g., Safer Internet Day
- Reference to the relevant web sites / publications such as www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers

Parents/ carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to the academy. **Please see Appendix 2.**
Parents/ carers are required to make a decision as to whether they consent to images of their child being taken/ used in the public domain (e.g., on an academy website). **Please see section 10.**

Education – The Wider Community
The academy will provide opportunities for local community groups / members of the community to gain from the academy's online safety knowledge and experience. This may be offered through the following:

- Online safety messages targeted towards grandparents and other relatives as well as parents.
- The school / academy website will provide online safety information for the wider community

4. Password Security
All users are responsible for implementing password security in all aspects of creating, protecting and managing passwords. Passwords for the academy systems must be created and managed in accordance with this policy. See **Appendix 3** for guidance

Password Disclosure
Users **must not** disclose their passwords to anyone.
Users **must not** write their passwords down under any circumstances.
Unauthorised password disclosure is deemed a serious security matter and may be dealt with under the academy's Disciplinary Procedure, up to and including termination of employment.

Shared Passwords
There may be rare occasions when it is necessary to share a common password between more than one user, if having individual usernames and passwords is operationally unacceptable, such as where the sharing of equipment is required, and the logout and login times required to swap users are unacceptable.
Any such arrangement **must** be authorised by the Headteacher
All access to line of business applications, including email, will be gained through the use of individual logins which will have to be entered by each user independently.

5 Data Security
The accessing of Academy data is something that we take very seriously.
Any data shared with an external body must be subject to a data sharing agreement approved by the Headteacher.
Staff must be made aware of their responsibilities when accessing academy data.
They **must not**:

- access data outside of the academy, except when entering/using assessment data;
- take copies of the data;
- allow others to view the data;
- Edit the data unless specifically requested to do so by the Headteacher and/ or the Local Academy Board;
- Leave Integris open for students to view;
- Leave their workstations unlocked when leaving the classroom;
- Allow a student to use the teacher laptop; and
- Share staff passwords or store passwords insecurely.

6. Cyber Security

Cyber-attacks are crimes against a school that need to be investigated so perpetrators can be found and counter-measures identified.

A cyber-attack is defined as an intentional and unauthorised attempt to access or compromise the data, hardware or software on a computer network or system. An attack could be made by a person outside or inside the school.

The National Cyber Security Centre define what a cyber incident is.

This compromise of data might include:

- stealing the data
- copying the data
- tampering with the data
- damaging or disrupting the data, or similar
- unauthorised access

Any suspicious cyber incident should be reported to the Executive Head/ Headteacherand they will make the decision to contact Action Fraud on 0300 123 2040 or on the Action Fraud website.

Police investigations may find out if any compromised data has been published or sold and identify the perpetrator.

7.Acceptable Usage

Effective security is a team effort involving the participation and support of every St Botolph’s employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

General Use and Ownership

While the Core Information Technology Services team (CITS) wishes to provide a reasonable level of privacy, users should be aware that the data or emails they create on the corporate systems remain the property of the academy. Because of the need to protect the network, management cannot guarantee the confidentiality of information stored on any network device belonging to the academy.

Employees are responsible for exercising good judgment regarding the reasonableness of personal use. If there is any uncertainty, employees should consult their line manager.

Any information that users consider sensitive or vulnerable must be encrypted. For guidelines on encrypting your information contact CITS.

For security and network maintenance purposes, authorised individuals within the academy may monitor equipment, systems and network traffic at any time.

The academy reserves the right to audit networks and systems on a periodic basis.

Unacceptable Use

The activities listed in **Appendix 4** are prohibited.

8. Managing the Internet Safely

The academy monitors Internet use from all computers and devices connected to the corporate network. For all traffic, the monitoring system must record the source IP Address, the date, the time, the protocol, and the destination site or server. Where possible, the system should record the User ID of the person or account initiating the traffic. Internet Use records must be preserved for one hundred and eighty 180 days.

Core Information Technology Services (CITS) members may access all reports and data if necessary to respond to a security incident. Internet Use reports that identify specific users, sites, teams, or devices will only be made available to associates outside the CITS upon written or email request to CITS from a Human Resources Representative. Further guidance on managing the internet safely is provided in **Appendix 5**

9 Managing Email

When using communication technologies, the academy considers the following as good practice:

- The official *academy* email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. *Staff and pupils should therefore use only the academy email service to communicate with others when in school, or on academy systems (e.g., by remote access).*
- Users must immediately report, to the nominated person – in accordance with the academy policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and pupils or parents / carers (email, social media, chat, blogs, VLE etc) must be professional in tone and content. *These communications may only take place on official (monitored) academy systems. Personal email addresses, text messaging or social media must not be used for these communications.*
- *Pupils will be taught about online safety issues, such as the risks attached to the sharing of personal details. They will also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.*
- *Personal information should not be posted on the academy website and only official email addresses should be used to identify members of staff.*
- Any breach of this E-Safety Policy may be dealt with under the academy's Disciplinary Procedure, up to and including termination of employment.

Personal Use.

Using a reasonable amount of academy resources for personal emails is acceptable, but non-work related email must be saved in a separate folder from work related email. Sending chain letters or joke emails from an academy email account is prohibited. Virus or other malware warnings and mass mailings from academy accounts must be approved by CITS before sending.

Monitoring

The academy may monitor messages without prior notice. They are not obliged to monitor email messages

Email Forwarding Policy

St Botolph's Academy employees are provided with an academy email account. Employees are not permitted to use personal email accounts for academy business. Unless approved by an employee's Line Manager, academy email will not be automatically forwarded to an external email address.

10 Social networking / Web Technologies

All schools, academies, MATs and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools/academies, MATs and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, engage in online bullying, discriminate on the grounds of sex, race or disability or who defame a third party may render the *academy* or local authority / MAT liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The academy provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through:

- Ensuring that personal information is not published
- Training is provided including: acceptable use; social media risks; checking of settings; data protection; reporting issues
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

Academy staff should ensure that:

- No reference should be made in social media to pupils, parents / carers or academy staff
- They do not engage in online discussion on personal matters relating to members of the a community
- Personal opinions should not be attributed to the *academy* or local authority / MAT
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information

When official academy social media accounts are established, there should be:

- *A process for approval by senior leaders*
- *Clear processes for the administration and monitoring of these accounts – involving at least two members of staff*
- *A code of behaviour for users of the accounts, including*
- *Systems for reporting and dealing with abuse and misuse*
- *Understanding of how incidents may be dealt with under academy disciplinary procedures*

Personal Use:

- Personal communications are those made via a personal social media account. In all cases, where a personal account is used which associates itself with the academy or impacts on the academy, it must be made clear that the member of staff is not communicating on behalf of the academy with an appropriate disclaimer. Such personal communications are within the scope of this policy
- Personal communications which do not refer to or impact upon the academy are outside the scope of this policy
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken

Monitoring of Public social media

- As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the school
- The school should effectively respond to social media comments made by others according to a defined policy or process

St Botolph’s Academy does not discourage staff and students from using such services in their own time. However, all should be aware that the Local Academy Board will take seriously any occasions where the services are used inappropriately. It is important to recognise that there are also issues regarding the appropriateness of some content, contact, culture and commercialism. To this end, we encourage staff and students to think carefully about the way that information can be added and removed by all users, including themselves, from these sites. Additional guidance for both staff and students is included in **Appendix 6.**

Any serious misuse of Social Networking sites will be dealt with in accordance with the academy Disciplinary policy.

Guidance is provided below in respect of Facebook and X. The same principles should be applied to other social networking sites such as WhatsApp and Snapchat. This list is not exhaustive.

Facebook

The Local Academy Board of St Botolph's Academy advises that employees do not have Facebook accounts.

However, staff who choose to do so may use Facebook in their own time using their own IT assets. But:

- Under no circumstances should pupils or ex-pupils under the age of 18 be accepted as a friend. Failure to follow this will result in disciplinary action being taken. If a child requests a member of staff as a friend, then the child's parents must be informed
- Staff are asked to use extreme caution if a parent makes contact through Facebook. In the event of communicating with a parent or adult associated with a child who attends the school, an employee must not make any comments about students, staff or parents
- Any statements or status remarks must not contain any comments about the academy, staff, parents or students
- Teaching Staff should not use St Botolph's equipment to access social networking sites as part of their work unless prior permission has been granted by their line manager

10.2 X

The academy may use X social networking as a method of communication with stakeholders. This communication is permitted by the Local Academy Board providing it adheres to the following guidelines.

- The Headteacher is responsible for the content of an a Twitter feed, should it have one
- The Twitter feed must be used for academy business only. The content must be appropriate and considered
- Access to the academy Xaccount will be managed by the Headteacher with an authorised user list available to Governors on request
- An administration account for all academy X feeds should be submitted to the Headteacher upon request
- Inappropriate content posted via X will result of suspension of the account and control of the account will be taken by the academy.

11. Cyber Bullying

What is cyberbullying?

Cyberbullying is bullying online and any form of anti-social behaviour over the internet or via a mobile device. It is an attack or abuse, using technology, which is intended to cause another person harm, distress or personal loss.

Forums and tools used often vary and include a range of electronic devices often linked to forums or chat rooms. The tool may be a computer or laptop, a mobile phone, a camera or recording device, a tablet or games-console or simply email or mobile text messaging. Typically, the bullies use social networking sites such as Facebook, X and other interactive forums to target an individual or group. Some examples of cyberbullying can include: individual or group. Some examples of cyberbullying can include:

- Spreading malicious and abusive rumours and gossiping
- Emailing or texting you with threatening or intimidating remarks
- Mobbing (a group or gang that target you)
- Harassing you repeatedly
- Intimidation and blackmail
- Stalking you online and continually harassing you
- Posting embarrassing or humiliating images or videos without your consent.
- Posting your private details online without consent
- General bullying or stalking
- Grooming (enticing or goading you online to self-harm or commit a crime
- Setting up a false profile, identity fraud or identity theft
- Using gaming sites to attack or bully you
- Theft, fraud or deception over the internet.

All concerns over cyberbullying should be referred to the relevant teacher/DSL.

12. Online Sexual Harassment

Online sexual harassment is defined as unwanted sexual conduct on any digital platform. It includes a wide range of behaviours that use technology to share digital content such as images, videos, posts, messages, pages etc. on a variety of different platforms (private or public). This includes adult to child or child to child.

There are four main types of online sexual harassment. These different behaviours are often experienced simultaneously and can overlap with offline experiences of sexual harassment. These are

- non-consensual sharing of intimate images and videos
- exploitation, coercion and threats
- sexualised bullying
- unwanted sexualisation

Further information on sexual harassment can be found in our safeguarding policy and all concerns over sexual harassment should be referred to a DSL.

13 Safe Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The academy will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff will inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g., on social networking sites.

- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow the academy's policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school / academy equipment, the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that students / pupils are appropriately dressed and are not participating in activities that might bring the individuals or the academy into disrepute. If you believe that an inappropriate photograph has been taken, do not view the photograph, contact a DSL as soon as possible with the device.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of students; this includes when on field trips. However, with the express permission of the Headteacher, images can be taken provided they are transferred immediately and solely to the academy's network and deleted from the staff device.
- Consent of adults who work at the academy - Permission to use images of all staff who work at the academy should be sought on induction and a copy retained in the individual's personnel file

Publishing pupil's images and work

On a child's entry to the academy, parents/guardians will be asked to give permission to use their child's work/photos in the following ways on the academy web site;

- in the academy prospectus and other printed publications that the academy may produce for promotional purposes;
- recorded/ transmitted on a video or webcam;
- in display material that may be used in the academy's communal areas;
- in display material that may be used in external areas e.g., an exhibition promoting the academy; and
- general media appearances, e.g., local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically.)

This consent form is considered valid for the entire period the child attends the academy unless there is a change in the child's circumstances where consent could be an issue, e.g., divorce of parents, custody issues, etc.

Parents/ carers may withdraw permission, in writing, at any time. Consent has to be given by the person with parental responsibility to be valid.

Students' full names will not be published alongside their image. Email and postal addresses of students will not be published. Before posting student work on the Internet, a check needs to be made to ensure that permission has been given for work to be displayed. No photos should be uploaded to website or put in any publications without prior checking with the Headteacher or nominated responsible person at the academy**.**

Only the academy, or the nominated responsible person at the academy has authority to upload images to the site. **If links to YouTube are provided a disclaimer must state that this link is to an external website and that the academy is not responsible for the content of external sites.**

Storage of Images

Images/ films of children are stored on the academy's network.
Students and staff are not permitted to use personal portable media for storage of images (e.g., USB sticks) without the express permission of the Headteacher.
Rights of access to this material are restricted to the teaching staff and students within the confines of the academy network/ Learning Platform.

Webcams and CCTV

Please see the academy **CCTV policy**.

Video Conferencing

Video conferencing can provide valuable leaning opportunities but the associated risks need to be carefully considered and managed**. Appendix 7** provides specific guidance in respect of the use of video conferencing by Academies

14 Remote Access

Mobile computing and storage devices containing or accessing the information resources at the academy must be approved by CITS prior to connecting to the academy information systems. This applies to all devices connecting to the network at THE ACADEMY, regardless of ownership.
Mobile computing and storage devices include, but are not limited to: laptop computers, personal digital assistants (PDAs), plug-ins, Universal Serial Bus (USB) port devices, Compact Discs (CDs), Digital Versatile Discs (DVDs), flash drives, modems, handheld wireless devices, wireless networking cards, and any other existing or future mobile computing or storage device, either personally owned or academy owned, that may connect to or access the information systems at the academy.
A risk analysis for each new media type must be conducted and documented prior to its use or connection to the network at the academy.

15 Mobile technologies, including Removable Media Devices

Removable media devices, including laptops, mobile phones, tablets and USB memory sticks are particularly vulnerable to loss and theft due to their size and portability. Users must take all reasonable precautions to prevent a security breach. Approval for access to, and use of, mobile computing and removable media devices must be given by your line manager or CITS. Should access to, and use of, mobile computing and removable media devices be approved, the following sections apply and must be adhered to at all times.
Special care **must** be taken to physically protect the removable media device and stored information from loss, theft or damage. Anyone using removable media devices to transfer information must consider the most appropriate way to transport the device and be able to demonstrate that they took reasonable care to avoid damage or loss.
Only information that is authorised and necessary to be transferred should be saved on to the removable media device. Users should note that information that has been deleted can still be retrieved.
Removable media devices **must not** be used for archiving or storing records as an alternative to other storage equipment.

Non-academy owned removable media devices **must not** be used to store any information used to conduct official academy business, and **must not** be used with any academy owned or leased IT equipment unless authorised by the academy.
Further detailed guidance is provided in **Appendix 8**.

It should be noted that if a user loses or has a mobile device/tablet stolen which contains unencrypted personal data owned by the academy, they may be liable to prosecution under the Data Protection Act 1998.

16 Misuse or Infringements

Inappropriate material

All users must be made aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the member of SLT/DSL. The member of SLT/DSL must record the incident on CPOMS. **Please see Appendix 9.** This incident log must be monitored termly by the Executive Head/ Headteacherl, designated SLT member or Chair of the Local Academy Board.
Deliberate access to inappropriate materials by any user will lead to the incident being logged by a member of SLT/DSL. Depending on the seriousness of the offence further action taken may include:

- investigation by the Executive Head/ Headteacher / Local Academy Board;
- immediate sanctions, possibly leading to exclusion/dismissal; or
- involvement of police for very serious offences.

Users are made aware of sanctions relating to the misuse or misconduct through inductions (staff) and computing lessons (students).

17 Anti-Virus

All academy PCs must have the the academy's's standard, supported anti-virus software installed and scheduled to run at regular intervals. In addition, the anti-virus software and the virus pattern files must be kept up-to-date. Virus-infected computers must be removed from the network until they are verified as virus-free. Academy Technical Leads are responsible for creating procedures that ensure anti-virus software is run at regular intervals, and computers are verified as virus-free. Any activities with the intention to create and/or distribute malicious programs into the academy'snetworks (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.) are prohibited.

18 Computer Use

Appropriate measures must be taken when using computers to ensure the confidentiality, integrity and availability of sensitive information and that access to sensitive information is restricted to authorised users.
Employees using computers must consider the sensitivity of the information that may be accessed and minimise the possibility of unauthorised access.
Appropriate measures include:

- Restricting physical access to computers to only authorised personnel;
- Securing computers (screen lock or logout) prior to leaving an area to prevent unauthorised access;
- Enabling a password-protected screen saver with a short timeout period to ensure that computers that were left unsecured will be protected;
- Ensuring computers are used for authorised business purposes only;
- Never installing unauthorised software on computers; and

- Ensuring that monitors are positioned away from public view. If necessary, privacy screen filters or other physical barriers to public viewing will be installed.

19 Clear Screen

All users are expected to log off from their PCs/ laptops when left for long periods and overnight.

When leaving their desk for lunch or to attend a meeting, users should lock down their screen using Ctrl, Alt, Del and then selecting Lock Workstation. The academy systems will do this automatically after 15 minutes; however, taking this measure will further reduce any security risk. **NOTE: The academy may need longer than 15 minutes to cover timeout during lessons. This should be discussed and agreed with CITS before implementation.**

Mobile devices through which access to the network can be obtained, for example iPad, should be PIN protected, set to power off after a period of within 5 minutes and switched off when left unattended. These devices should be stored securely when not in use.

20 Complaints

Complaints relating to e-safety should be made to the Executive Head/ HeHeadteacher/DSL. E safety incidents should be recorded using CPOMS

21 Review

This policy will be reviewed every three years, or when there are changes to relevant legislation.

St Botolph's CE Academy
Acceptable Use Agreement
For St Botolph's Academy Staff, Local Academy Board and Visitors

Computing and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in the Trust and its Academies. All staff are expected to sign this agreement and adhere at all times to its contents. Any concerns or clarification should be discussed with a member of the SLT.

- I will only use the academy's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Headteacher /Executive Head or Local Academy Board.
- I will comply with the computing system security and not disclose any passwords provided to me by the academy or other related authorities.
- I will ensure that all electronic communications with students and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number and personal email address, to students.
- I will only use the approved, secure email system(s) for any academy business.
- I will ensure that personal data (such as data held on Arbour) is kept secure and is used appropriately, whether in the academy, taken off the academy premises or accessed remotely. Personal data can only be taken out of the academy or accessed remotely when authorised by the Head of School/Executive Head or the Local Academy Board.
- I will not install any hardware of software without permission of the ICT technician.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of students and/ or staff will only be taken, stored and used for professional purposes in line with academy policy and with the written consent of the parent, carer or staff member. Images will not be distributed outside the academy network without the permission of the parent/ carer, member of staff or Headteacher/Executive Head.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Headteacherl/Executive Head.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in and outside the academy, will not bring my professional role into disrepute.
- I will support and promote the academy's E-Safety policy and help students to be safe and responsible in their use of ICT and related technologies.

User Signature

I agree to follow this Acceptable Use Agreement and to support the safe use of ICT throughout the academy.

Signature …………………………………… Date ……………………

Full Name ……………………………….....................(printed)

Job title . . . .

Appendix 2
St Botolph's C of E Academy

Acceptable Use Agreement

Acceptable Use Agreement / E-Safety Rules for KS2 pupils/parents

- I will only use ICT systems in the academy, including the internet, email, digital video, mobile technologies, etc. for academy purposes.
- I will not download or install software on a technologies.
- I will only log on to the academy network/ Learning Platform with my own user name and password.
- I will follow the academy's ICT security system, will not reveal my passwords to anyone and will change them regularly.
- I will only use my academy email address while at the academy or while using the academy's equipment.
- I will make sure that all ICT communications with students, teachers or others is responsible and sensible.
- I will be responsible for my behaviour when using the Internet. This includes resources I access and the language I use.
- I will not deliberately browse, download, upload or forward material that could be considered offensive or illegal. If I accidentally come across any such material, I will report it immediately to my teacher.
- I will not give out any personal information such as name, phone number or address. I will not arrange to meet someone unless this is part of an aproject approved by my teacher.
- Images of students and/ or staff will only be taken, stored and used for academy purposes in line with academy policy and not be distributed outside the academy network without the permission of the Executive Head/ Headteacher.
- I will ensure that my online activity, both in and outside the academy, will not cause my academy, the staff, students or others distress or bring it into disrepute.
- I will only use my own technology in the academy as part of a pre-arranged education activity, with permission from a member of staff and authorised by the academy, this includes 4G/5G smart technologies.
- I will respect the privacy and ownership of others' work on-line at all times.
- I will not attempt to bypass the internet filtering system.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available to my teachers.
- I understand that these rules are designed to keep me safe and that if they are not followed, academy sanctions will be applied and my parent/ carer or the Police may be contacted.

Student Signature

I agree to follow this Code of Conduct and to support the safe use of ICT throughout the academy.

Signature …….…………………….………… Date ……………………
Full Name …………………………………....................................(printed) Year.

Appendix 3
Password characteristics and guidelines

Passwords **must** be composed of the following characteristics:

- The password is at least **eight (8)** alphanumeric characters long for non-critical and non-admin accounts.
- Critical Systems/user password should not be less than **fifteen (15)** alphanumeric characters (e.g., Built-in Admins, domain admins, and service accounts) whenever possible.
- The password must contain both upper and lower case characters (e.g., a-z, A-Z)

The password must contain at least one numeric digit (e.g., 0-9). Passwords **should NOT** have the following characteristics:

- A word found in a dictionary or a word in any language, slang, dialect, jargons etc.
- Passwords shall not be the same as the username, login id, or Payroll number.
- Default or generic passwords should not be used.
- Passwords with common usage words such as: Password, Letmein etc.
- Common names, family, pets, friends, co-workers, celebrities, famous historical figures…etc.
- Computer terms and names, commands, sites, companies, hardware, software.
- Personal information, addresses, birthdays, email, phone number etc.
- Patterns such as abcdef, ASDFGH, zyxwvuts, 123321, 123456, 98765 etc.
- Any of the above spelled backwards.
- Any of the above preceded or followed by a digit (e.g., secret1,1secret)

Creating memorable passwords:

- One way to do this is by creating a password based on a song title, poems, affirmation, or other common phrase. (e.g., the phrase might be: "This May Be One Way to Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

Password Expiry

All staff passwords will be forced to expire after **seventy-two (72) d**ays when possible. Password expiry notifications will be generated prior to expiry with ample time (at least **3 days** or at most **6 logins**) and reminders to change when possible. Passwords cannot be changed by the user until they are more than **one (1)** day old. Repetitive password change by the user within the same day should be disabled when possible, to prevent password history breaches

User Account Lockout

User accounts will be locked out for **fifteen (15)** minutes if **five (5**) incorrect passwords are entered.

For certain secured applications passwords may be changed when user access accounts are locked out more than **one (1)** time per **thirty-six (36)** hour period.

Password Reset

A user requiring a password reset for access to the standard academy desktop must contact the CITS (Core IT Services) and provide sufficient detail to assure the service desk that their request is genuine.

A user requiring a password reset for access to a secured system must contact the CITS Service Desk, which may request further authorisation from the user department or system administration team dependant on the security policy for that particular application.

When the user uses the password provided by the ICT Service Desk they **MUST** change the password immediately at the next login.

Password History

Users may not re-use passwords they have previously used when their password expires. The password history will be the minimum of **twenty (20)** passwords when possible.

If the CITS Service Desk needs user/desktop access so that they can gain physical access for work such as application installation or reimaging they will reset the password to a temporary one. Once the Service Desk team have completed their investigations they will inform the user of the temporary password which will have been set to expire at next login. The user should use the temporary password and change it immediately at the next login.

Authentication Mechanisms

Information systems will authenticate all users. Passwords will be used as a base level of authentication. Functions with high privilege and risk require strong multi-factor authentication, involving a password as well as one or more different authentication factors. Authentication options include hardware tokens, smartcards, alternative channels e.g. Public Key Infrastructure, (PKI), Certificates, Short Message Service (SMS), or call-back, one-time passwords and biometrics.

Password Entry (Network Security)

Information systems **must not** retain account or password information from previous logins.

Passwords **must not** be shown as plain-text when they are entered by a user. A common masking symbol (e.g. asterisk) shall be displayed for every typed character.

All production system-level passwords **must** be part of the administered global password management system.

User accounts that have system-level privileges granted through group memberships or programs such as "sudo" **must** have a unique password from all other accounts held by that user.

Single Sign On (SSO)

Single Sign On (SSO) provides the mechanism of accessing multiple systems with one access. However, secure systems, or systems with higherlevel data should always require a separate authentication, and **must not** be accessed via SSO.

Appendix 4
Unacceptable use
Under no circumstances is an employee of the academy authorised to engage in any activity that is illegal under UK or international law while utilising academy-owned resources.
The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

System and Network Activities
The following activities are strictly prohibited, with no exceptions:

- Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by THE ACADEMY/the academy.
- Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which THE ACADEMY or the end user does not have an active license.
- Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
- Introduction of malicious programs into the network or server (e.g. viruses, worms, Trojan horses, e-mail bombs, etc.).
- Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
- Using an academy computing asset to engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws.
- Making fraudulent offers of products, items, or services originating from any academy account.
- Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
- Port scanning or security scanning is expressly prohibited unless prior notification to the academy is made.

Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.

- Circumventing user authentication or security of any host, network or account.

- Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).

- Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.

- Providing information about, or lists of, the academy’s employees to outside parties.

Email and Communications Activities
The following activities are strictly prohibited, with no exceptions:

- Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).

- Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.

- Unauthorized use, or forging, of email header information.

- Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.

- Use of unsolicited email originating from within the academy’snetworks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by the academy or connected via the academy network.

- Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

Appendix 5

Internet Use Filtering System

CITS will block access to Internet websites and protocols that are deemed inappropriate for the academy's environment. The following protocols and categories of websites will be blocked:

- Adult/Sexually Explicit Material;
- Advertisements & Pop-Ups;
- Chat and Instant Messaging;
- Gambling;
- Hacking;
- Illegal Drugs;
- Intimate Apparel and Swimwear;
- Peer to Peer File Sharing;
- Personals and Dating;
- Social Network Services;
- SPAM, Phishing and Fraud;
- Spyware;
- Tasteless and Offensive Content;
- Violence, Intolerance and Hate; and
- Certain, non-approved, Web Based Email.

Internet Use Filtering Rule Changes

The CITS will periodically review and recommend changes to web and protocol filtering rules. Changes to web and protocol filtering rules will be recorded in CITS protocols and will be available on request to employees of the academy. A member of the DSL team will run regular checks on a range of devices on the academy network to ensure the filtering system is up to date and efficient in blocking words/searches that they deem inappropriate. This information will then be forwarded onto our IT team to add any additional words.

Internet Use Filtering Exceptions

If a site is mis-categorised, employees may request the site be un-blocked by submitting a change request to CITS. CITS will review the request and un-block the site if it is mis-categorised.

Employees may access blocked sites with permission if access is appropriate and necessary for business purposes. If an employee needs access to a site that is blocked and appropriately categorized, they must submit a request to their Human Resources representative or Line Manager. All requests for approval of a site must be made in writing or by email to CITS

Appendix 6 Social Networking

Students

- All students are advised to be cautious about the information given by others on sites, for example users not being who they say they are.
- Students should avoid placing images of themselves (or details within images that could give background details) on such sites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online.
- Students are always reminded to avoid giving out personal details on such sites which may identify them or where they are (full name, address, mobile/ home phone numbers, academy details, IM/ email address, specific hobbies/ interests).
- Students are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.
- Students are encouraged to be wary about publishing specific and detailed private thoughts online.
- Our students are asked to report any incidents of bullying to a member of staff at the academy.

Employees

- Staff may only create blogs, wikis or other web 2 spaces in order to communicate with students using the VLE or other systems approved by the Executive Head/ Headteacher.
- An individual is free to talk about the academy. However instances of the academy being brought into disrepute may constitute misconduct or gross misconduct and disciplinary action will be taken.
- An employee must not disclose confidential information relating to his/her employment at the academy.
- Sites must not be used to verbally abuse staff or students. Privacy and feelings of others should be respected at all times. Employees should obtain the permission of individuals before posting contact details or pictures. Care should be taken to avoid using language which could be deemed as offensive to others.
- If information on the site raises a cause for concern with regard to any conflict of interest, employees should raise the issue with their line manager.
- If approached by a media contact about content on a site relating to the academy, employees should advise their line manager before taking any action.
- Viewing and updating personal sites must not take place during working hours unless agreed in advance as appropriate by the Line Manager.
- Sites must not be used for accessing or sharing illegal content. Blogging from the academy’s systems is subject to monitoring

Appendix 7

Video Conferencing – guidance

Permission is sought from parents and carers if their children are involved in video conferences.

Permission is sought from parents and carers if their children are involved in video conferences with end-points outside of the academy.

All students are supervised by a member of staff when video conferencing.

All students are supervised by a member of staff when video conferencing with end-points beyond the academy.

The academy keeps a record of video conferences, including date, time and participants.

Approval from the Headteacher is sought prior to all video conferences within the academy.

The academy conferencing equipment is not set to auto-answer and is only switched on for scheduled and approved conferences.

No part of any video conference is recorded in any medium without the written consent of those taking part.

Additional points to consider:

- Participants in conferences offered by 3rd party organisations may not be DBS checked.
- Conference supervisors need to be familiar with how to use the video conferencing equipment, particularly how to end a call if at any point any person taking part becomes unhappy with the content of the conference

Appendix 8
Mobile technologies – guidance
Laptops
In order to minimise the potential risks, users must apply the following security controls:

- The physical security of laptops is the personal responsibility of users who must take all reasonable precautions and be sensible and stay alert to the risks.
- Users **must** keep laptops within their possession within sight whenever possible. They should never be left unattended in public view. Extra care should be taken in public places such as airports, railway stations or restaurants.
- Where possible, laptops should be locked out of sight and must never be left unattended in a vehicle in public view. If absolutely necessary, it should be locked out of sight in the boot but it is generally safer for the user to take it with them.
- Laptops should be carried and stored in a padded laptop computer bag or strong briefcase to reduce the chance of accidental damage. An ordinary-looking briefcase is also less likely to attract thieves than an obvious laptop bag.
- In the event of loss or theft the Executive Head/ Headteachermust be notified immediately and the academy Core IT Service Desk informed as soon as practicable. They may choose to call the police.
- Information should not be stored on local hard drives unless there is no alternative. Protectively marked information must not be stored on the hard drive unless it is encrypted.
- Data encryption may be applied to all laptop hard drives owned by the academy.

Tablets, mobile phones and USB Sticks
These remain the property of the academy. In order to minimise any potential risks, users must apply the following security controls:

- Personal devices **must not** be connected to a laptop or desktop for any other purpose than re-charging the device.
- No protectively marked information may be stored on a mobile device unless it is encrypted and the device is locked with a PIN code.
- It is the user's responsibility to ensure that sensitive information, including that contained in emails, is not be held on a mobile device for longer than is necessary.
- All spam, chain and other junk emails are subject to the the academy's email policy.
- The downloading of unauthorised software on to an academy/ device is prohibited.
- Employees **must** report any suspected virus to the the academy Core ICT Service desk immediately.

Employees must take all appropriate steps to protect the mobile device from loss, theft or damage. These steps include, but are not limited to:-

- The mobile device **must not** be left unattended in public view in a vehicle,
- The mobile device **must not** be left unattended in a public place.
- The keypad **must** be locked at all times when the mobile device is not in use.

- All mobile devices **must** be password/pin protected.
- Users should be aware that the academy may deploy software to monitor the use of removable media devices and the transfer of information to and from all removable media devices and academy-owned IT equipment. Management reports may be generated and used to support internal and external audit.
- Damaged, faulty or infected devices must not be used.
- Up-to date virus and malware checking software must be operational on both the machine from which the information is taken and the machine on to which the data is to be loaded. In order to implement this, it is necessary to regularly plug laptops into the the academy network.
- If whilst using removable media the checking software indicates there is a problem, use of the device must be stopped immediately and the academy Core ICT Services informed so it can be recorded as an incident.

Appendix 9

Date and Time
Actions and reasons

Details of all e-Safety incidents to be recorded by the E-Safety Coordinator. This incident log will be monitored termly by the Headteacher, member of SLT or Chair of the Local Academy Board.	**Name of pupil or staff member**	**Male or female**	**Room and computer / device number**	**Details of incident (including evidence)**