On-line Safety
and
Data Security Policy

May 2022

Policy Title	On-line Safety and Data Security
Policy Created / Amended	May 2022
Policy Ratified	May 2022
Policy review cycle	2 Years
Policy Review Date	May 2024

Introduction

ICT in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, Academies need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

Information and Communications Technology covers a wide range of resources including web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Apps
- E-mail, Instant Messaging and chat rooms
- Social Media, including Facebook, Snapchat and Twitter
- Mobile/smart phones with text, video and/or web functionality
- Other mobile devices including tablets and gaming devices
- Online games
- Learning Platforms and Virtual Learning Environments
- Blogs and Wikis
- Podcasting
- Video sharing
- Downloading
- On demand TV and video, movies and radio / Smart TVs.

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these internet technologies and that some have minimum age requirements (13 years in most cases).

At Sybil Andrews Academy, we understand the responsibility to educate our students on On-line Safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Academies hold personal data on learners, staff and others to help them conduct their day-to-day activities. Some of this information is sensitive and could be used by another person or criminal organisation to cause harm or distress to an individual. The loss of sensitive information can result in media coverage, and potentially damage the reputation of the Academy.

Everybody in the Academy community has a shared responsibility to secure any sensitive information used in their day-to-day professional duties and even staff not directly involved in data handling should be made aware of the risks and threats and how to minimise them.

Both this policy and the Acceptable Use Agreement (for all staff, governors, students and regular visitors for regulated activities) cover both fixed and mobile internet technologies provided by the Academy (such as PCs, laptops, mobile devices, webcams, whiteboards, digital video equipment etc.); and technologies owned by students and staff, but brought

onto Academy premises (such as laptops, mobile phones and other mobile devices).

Monitoring

Authorised ICT staff, the Head Teacher and Deputy Head Teachers will inspect any ICT equipment owned or leased by the Academy at any time without prior notice. If you are in doubt as to whether the individual requesting such access is authorised to do so, please ask for their identification badge and contact their department. Any ICT authorised staff member will be happy to comply with this request.

ICT authorised staff may monitor, intercept, access, inspect, record and disclose telephone calls, e-mails, instant messaging, internet/intranet use and any other electronic communications (data, voice, video or image) involving its employees, students or contractors, without consent, to the extent permitted by law. This may be to confirm or obtain Academy business related information; to confirm or investigate compliance with Academy policies, standards and procedures; to ensure the effective operation of Academy ICT; for quality control or training purposes; to comply with a Subject Access Request under the Data Protection Act 2018, or to prevent or detect criminal activity.

All monitoring, surveillance or investigative activities are conducted by ICT authorised staff and comply with the Data Protection Act 2018, the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000 (RIPA) and the Lawful Business Practice

Breaches

A breach or suspected breach of policy by an Academy employee, contractor or student may result in the temporary or permanent withdrawal of Academy ICT hardware, software or services from the offending individual.

For staff, any policy breach is grounds for disciplinary action in accordance with the Academy Disciplinary Procedure.

Policy breaches may also lead to criminal or civil proceedings.

Incident reporting

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the Academy's relevant responsible person. Additionally, all security breaches, lost/stolen equipment or data virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to the relevant responsible person. The relevant responsible individuals in the Academy are the ICT Support Team and the On-line Safety coordinator, Mr Ruffell.

Misuse and Infringements

Complaints

Complaints and/or issues relating to On-line Safety should be made to the On-line Safety co-ordinator or Headteacher. Incidents will be logged by the safety co-ordinator.

Inappropriate Material

All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the On-line Safety co-ordinator.

Deliberate access to inappropriate materials by any user will lead to the incident being logged by the relevant responsible person, and an investigation by the On-line Safety co-ordinator.

Depending on the seriousness of the offence, sanctions could include immediate suspension/ exclusion, possibly leading to dismissal/ permanent exclusion and involvement of police for very serious offences.

Computer viruses

- All files downloaded from the Internet, received via e-mail or on removable media such as a memory stick must be checked for any viruses using Academy provided anti-virus software before being used
- Never interfere with any anti-virus software installed on Academy ICT equipment
- If your machine is not routinely connected to the Academy network, you must make provision for regular virus updates through your ICT team
- If you suspect there may be a virus on any Academy ICT equipment, stop using the equipment and contact your ICT support provider immediately. The ICT support provider will advise you what actions to take and will be responsible for advising others that need to know.

Data Security

The accessing and appropriate use of Academy data is something that the Academy takes very seriously.

Security

- The Academy gives relevant staff access to it's Management Information System, with a unique username and password
- It is the responsibility of everyone to keep passwords secure
- Staff are issued with the relevant guidance documents and the Policy for ICT Acceptable Use
- Staff keep all Academy related data secure. This includes all personal, sensitive, confidential or classified data
- Staff should avoid leaving any portable or mobile ICT equipment or removable storage media in unattended vehicles. Where this is not possible, keep it locked out of sight
- Staff should always carry portable and mobile ICT equipment or removable media as hand luggage, and keep it under your control at all times
- It is the responsibility of individual staff to ensure the security of any personal, sensitive, confidential and classified information contained in documents faxed, copied, scanned or printed. This is particularly important when shared copiers (multi-function print, fax, scan and copiers) are used.

Email

The use of email within most schools is an essential means of communication for both staff and students. In the context of the Academy, email should not be considered private. Educationally, email can offer significant benefits including: direct written contact between schools on different projects, whether staff-based or student-based, within Academies or international. We recognise that students need to understand how to style an email in relation to their age and how to behave responsibly online.

Managing email

The Academy gives all staff & students their own email account to use for all Academy business as a work based tool This is to protect staff, minimise the risk of receiving unsolicited or malicious e-mails and avoids the risk of personal profile information being revealed. When using email:

- Staff & governors should use their Academy email for all professional communication & Academy business
- It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary email histories can be traced.
- Under no circumstances should staff contact students, parents or conduct any Academy business using personal email addresses
- All emails should be written and checked carefully before sending, in the same way as a letter written on Academy headed paper
- Students may only use Academy approved accounts on the Academy system for educational purposes
- Emails created or received as part of your Academy role will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000. You must therefore actively manage your email account as follows:
  - Delete all emails of short-term value
  - Organise email into folders and carry out frequent house-keeping on all folders and archives.
- All pupil email users are expected to adhere to the generally accepted rules of responsible online behaviour particularly in relation to: the use of appropriate language, not revealing any personal details about themselves or others in email communication, not arranging to meet anyone without specific permission, the use of virus checking attachments
- Students must immediately tell a member of staff if they receive an offensive or upsetting email
- Staff must inform the On-line Safety co-ordinator or line manager if they receive an offensive email
- However you access your Academy email (whether directly, through webmail when away from the office or on non-Academy hardware) all the Academy email policies apply.

Sending emails

- If sending emails containing personal, confidential, classified or financially sensitive data to external third parties or agencies, refer to the Section on emailing Personal, Sensitive, Confidential or Classified Information
- Use your own Academy e-mail account so that you are clearly identified as the originator of a message
- Keep the number and relevance of email recipients, particularly those being copied, to the minimum necessary and appropriate
- Do not send or forward attachments unnecessarily. Whenever possible, send the location path to the shared drive rather than sending attachments
- Academy email is not to be used for personal advertising.

Receiving emails

- Check your email regularly
- Activate your 'out-of-office' notification when away for extended periods
- Never open attachments from an untrusted source; consult your network manager first
- Do not use the email systems to store attachments. Detach and save business related work to the appropriate shared drive/folder
- The automatic forwarding and deletion of emails is not allowed

Emailing personal, sensitive, confidential or classified information

Where your conclusion is that email must be used to transmit such data, obtain express consent from your line manager to provide the information by email and exercise caution when sending the email and always follow these checks before releasing the email:

- Encrypt and password protect
- Verify the details, including accurate email address, of any intended recipient of the information
- Verify (by phoning) the details of a requestor before responding to email requests for information
- Do not copy or forward the email to any more recipients than is absolutely necessary
- Do not send the information to any person whose details you have been unable to separately verify (usually by phone)
- Send the information as an encrypted document **attached** to an e-mail
- Provide the encryption key or password by a **separate** contact with the recipient(s)
- Do not identify such information in the subject line of any email
- Request confirmation of safe receipt

Equal opportunities

Students with additional needs

The Academy endeavours to create a consistent message with parents/carers for all students and this in turn should aid establishment and future development of the Academy's On-line Safety rules.

However, staff are aware that some students may require additional support or teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of On-line Safety issues.

Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of On-line Safety. Internet activities are planned and well managed for these children and young people.

On-line Safety roles and responsibilities

As On-line Safety is an important aspect of strategic leadership within the Academy, the Head Teacher and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named On-line Safety co-ordinator in this Academy is Sarah Fisher who has been designated this role as a member of the Senior Leadership Team. All members of the Academy community have been made aware of who holds this post. It is the role of the On-line Safety co-ordinator to keep abreast of current issues and guidance through organisations such as Suffolk County Council, CEOP (Child Exploitation and Online Protection) and Childnet.

Senior Management and governors are updated by the Head Teacher/On-line Safety co-ordinator and all governors have an understanding of the issues and strategies at our Academy in relation to local and national guidelines and advice.

This policy, supported by the Academy's acceptable use agreements for staff, governors, visitors and students, is to protect the interests and safety of the whole Academy community. It is linked to the following mandatory Academy policies: child protection, health and safety, home–Academy agreements, and behaviour/pupil discipline (including the anti-bullying) policy and citizenship.

On-line Safety in the curriculum

ICT and online resources are increasingly used across the curriculum. We believe it is essential for On-line Safety guidance to be given to the students on a regular and meaningful basis. On-line Safety is embedded within our curriculum and we continually look for new opportunities to promote On-line Safety.

The Academy has a framework for teaching internet skills in meeting time.

Students are aware of the impact of Cyberbullying and know how to seek help if they are affected by any form of online bullying. Students are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e.

parent/carer, teacher/trusted staff member, or an organisation such as Cybermentors, Childline or CEOP report abuse button.

On-line Safety skill development for staff

New staff receive information on the Academy's acceptable use policy as part of their induction.

All staff have been made aware of their individual responsibilities relating to the safeguarding of children within the context of On-line Safety and know what to do in the event of misuse of technology by any member of the Academy community (see On-line Safety co-ordinator).

All staff are encouraged to incorporate On-line Safety activities and awareness within their curriculum areas and ensure they are adequately informed with up-to-date areas of concern.

Managing the Academy safety messages

- We endeavour to embed On-line Safety messages across the curriculum whenever the internet and/or related technologies are used
- The On-line Safety policy will be introduced to the students at the start of each Academy year
- On-line Safety posters will be prominently displayed
- The key On-line Safety advice will be promoted widely through Academy displays, newsletters, class activities and so on
- We will promote Safer Internet Day every February.

Internet access

The internet is an open worldwide communication medium, available to everyone, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people. All internet use through the Academy network is logged and the logs are randomly but regularly monitored. Whenever any inappropriate use is detected it will be followed up.

Managing the Internet

- The Academy provides students with supervised access to Internet resources (where reasonable) through the Academy's fixed and mobile internet connectivity

- Staff will preview any recommended sites, online services, software and apps before use

- Searching for images through open search engines is discouraged when working with students

- If internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher.

- All users must observe software copyright at all times. It is illegal to copy or distribute

Academy software or illegal software from other sources

- All users must observe copyright of materials from electronic resources

Internet use

- You must not post personal, sensitive, confidential or classified information or disseminate such information in any way that may compromise the intended restricted audience

- Do not reveal names of colleagues, students, others or any other confidential information acquired through your job on any social networking site or other online application

- On-line gambling or gaming is not allowed on Academy ICT equipment

It is at the Head Teacher's discretion as to what internet activities are permissible for staff and students and how this is disseminated.

Infrastructure

- Our Academy also employs some additional web-filtering which is the responsibility of Head ICT Technician.

- Sybil Andrews Academy is aware of its responsibility when monitoring staff communication under current legislation and takes into account: The Data Protection Act 2018, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2018, Regulation of Investigatory Powers Act 2000, Human Rights Act 1998

- Staff and students are aware that Academy based email and internet activity can be monitored and explored further if required

- The Academy uses management control tools for controlling and monitoring workstations

- If staff or students discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the e-safety coordinator or teacher as appropriate

- It is the responsibility of the Academy, by delegation to the network manager and staff to ensure that anti-virus protection is installed and kept up-to-date on all Academy machines

- Students and Staff using personal removable media are responsible for measures to protect against viruses, for example making sure that additional systems used have up-to-date virus protection software. It is not the Academy's nor the network manager's responsibility to install or maintain virus protection on personal systems. If students wish to bring in work on removable media it must be given to an ICT Technician for a safety check first

- If there are any issues related to viruses or anti-virus software, the network manager/ ICT support team should be informed by email

Managing other online technologies

Online technologies, including social networking sites, if used responsibly both outside and within an educational context can provide easy to use, creative, collaborative and free facilities. However it is important to recognise that there are issues regarding the appropriateness of some content, contact, culture and commercialism. To this end, we encourage our users to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.

- At present, the Academy endeavours to deny access to social networking and online games websites from within the Academy
- All students are advised to be cautious about the information given by others on such websites, for example users not being who they say they are
- Students are taught to avoid placing images of themselves (or details within images that could give background details) on such websites 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 websites which may identify them or where they are (full name, age, address, mobile/ home phone numbers, Academy details, IM/email address, specific hobbies/interests)
- Our students are advised to set and maintain their online profiles to maximum privacy and deny access to unknown individuals
- Students are encouraged to be wary about publishing specific and detailed private thoughts and information online
- Our students are asked to report any incidents of cyberbullying to the Academy
- Staff may only create blogs, wikis or other online areas in order to communicate with students using the Academy learning platform or other systems approved by the Head Teacher
- Services such as Facebook and Instagram have a 13+ age rating which should not be ignored http://www.coppa.org/comply.htm

Parental involvement

We believe that it is essential for parents/carers to be fully involved with promoting On-line Safety both in and outside of the Academy and to be aware of their responsibilities.

- Parents/carers and students are actively encouraged to contribute to adjustments or reviews of the Academy On-line Safety policy consultation at parents forum
- Parents/carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to the Academy
- Parents/carers are required to make a decision as to whether they consent to images of their child being taken and used in the public domain (e.g. on Academy website)
- The Academy disseminates information to parents relating to On-line Safety where appropriate in the form of:
    - Academy website information
    - Newsletter items

Passwords

Password security

Password security is essential for staff, particularly as they are able to access and use student data. Staff are expected to have secure passwords which are not shared with anyone. They are expected to change these regularly. The students are expected to keep their passwords private and not to share with others, particularly their friends. Staff and students are regularly reminded of the need for password security.

All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the Academy's e-Safety Policy and Data Security.

Students are not allowed to deliberately access on-line materials or files on the Academy network or local storage devices of their peers, teachers or others.

Staff are aware of their individual responsibilities to protect the security and confidentiality of the Academy networks, MIS systems and/or learning platform, including ensuring that passwords are not shared and are changed periodically. Individual staff users must also make sure that workstations are not left unattended and are locked.

In our Academy, all ICT password policies are the responsibility of the Head Teacher and all staff and students are expected to comply with the policies at all times.

Password Dos and Don'ts

- **Always use your own** personal passwords
- Make sure you enter your personal passwords each time you logon. Do not include passwords in any automated logon procedures
- Staff should change temporary passwords at first logon
- Change passwords whenever there is any indication of possible system or password compromise
- Do not record passwords or encryption keys on paper or in an unprotected file
- **Only disclose your personal password to authorised ICT support staff when necessary, and never to anyone else**. Ensure that all personal passwords that have been disclosed are changed once the requirement is finished
- **Never tell a child or colleague your password**
- **If you are aware of a breach of security with your password or account inform an ICT technician immediately**
- Passwords must contain a minimum of six characters and be difficult to guess
- Passwords should contain a mixture of upper and lowercase letters, numbers and symbols

If you think your password may have been compromised or someone else has become aware of your password report this to your ICT support team.

Remote access

- You are responsible for all activity via your remote access facility
- Only use equipment with an appropriate level of security for remote access

- To prevent unauthorised access to Academy systems, keep all dial-up access information such as telephone numbers, logon IDs and PINs confidential and do not disclose them to anyone
- Select PINs to ensure that they are not easily guessed, eg do not use your house or telephone number or choose consecutive or repeated numbers
- Avoid writing down or otherwise recording any network access information. Any such information that is written down must be kept in a secure place and disguised so that no other person will be able to identify what it is
- Protect Academy information and data at all times, including any printed material produced while using the remote access facility. Take particular care when access is from a non-Academy environment

Safe use of images

Taking of images and film

Digital images are easy to capture, reproduce and publish and, therefore, misuse. We must remember that it is not always appropriate to take or store images of any member of the Academy community or public, without first seeking consent and considering the appropriateness.

- With the written consent of parents/carers (on behalf of students) and staff, the Academy permits the appropriate taking of images by staff and students with Academy equipment
- 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 Head Teacher, images can be taken provided they are transferred immediately and solely to the Academy's network and deleted from the staff device
- Students are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of students, staff and others without advance permission from the Head Teacher
- Students and staff must have permission from the Head Teacher before any image can be uploaded for publication

Consent of Adults who work at the Academy

Permission to use images of all staff who work at the Academy is sought on induction.

Publishing Pupil's Images and Work

On a child's entry to the Academy, all parents/carers 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
- On the Academy's learning platform or Virtual Learning Environment
- In display material that may be used in the Academy's communal areas

- In display material that may be used in external areas, ie exhibition promoting the Academy
- General media appearances, eg 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 that the child attends this Academy unless there is a change in the child's circumstances where consent could be an issue, eg divorce of parents, custody issues, etc.

Parents or carers may withdraw permission, in writing, at any time. Consent must also be given in writing and will be kept on record by the Academy.

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.

Stored 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 Head Teacher.

Rights of access to this material are restricted to the teaching staff and students within the confines of the Academy network or other online Academy resources.

Webcams

Webcams will not be used for broadcast on the internet without prior parental consent.

Misuse of the webcam by any member of the Academy community will result in sanctions (as listed under the 'inappropriate materials' section of this document).

Webcams include any camera on an electronic device which is capable of producing video. Academy policy should be followed regarding the use of such personal devices.

Video Conferencing

- Permission is sought from parents and carers if their children are involved in video conferences with end-points outside of the Academy/ Trust
- All students are supervised by a member of staff when video conferencing
- The Academy keeps a record of video conferences, including date, time and participants
- Approval from the Head Teacher is sought prior to all video conferences within Academy to end-points beyond 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 from parents/carers.

Academy ICT Equipment including Portable & Mobile ICT Equipment & Removable Media

Academy ICT Equipment

- As a user of the Academy ICT equipment, you are responsible for your activity
- It is recommended that Academies log ICT equipment issued to staff and record serial numbers as part of the Academy's inventory
- The Academy does not allow your visitors to plug their ICT hardware into the Academy network points (unless special provision has been made). They should be directed to the wireless ICT facilities if available
- Ensure that all ICT equipment that you use is kept physically secure
- Do not attempt unauthorised access or make unauthorised modifications to computer equipment, programs, files or data. This is an offence under the Computer Misuse Act 1990
- It is imperative that you save your data on a frequent basis to the Academy's network. You are responsible for the backup and restoration of any of your data that is not held on the Academy's network
- Personal or sensitive data should not be stored on the local drives of desktop PC, laptop, USB memory stick or other portable device. If it is necessary to do so the local drive must be encrypted
- It is recommended that a time locking screensaver is applied to all machines. Any device accessing personal data must have a locking screensaver as must any user profiles
- Privately owned ICT equipment should not be used on a Academy network
- On termination of employment, resignation or transfer, return all ICT equipment to your line manager. You must also provide details of all your system logons so that they can be disabled
- It is your responsibility to ensure that any information accessed from your own PC or removable media equipment is kept secure, and that no personal, sensitive, confidential or classified information is disclosed to any unauthorised person
- All ICT equipment allocated to staff must be authorised by the appropriate Line Manager. Authorising Managers are responsible for:
    - maintaining control of the allocation and transfer within their unit
    - recovering and returning equipment when no longer needed

Portable & Mobile ICT Equipment

This section covers such items as laptops, mobile devices and removable data storage devices. Please refer to the relevant sections of this document when considering storing or transferring personal or sensitive data

- All activities carried out on Academy systems and hardware will be monitored in accordance with the general policy
- Staff must ensure that all Academy data is stored on the Academy network, and not kept solely on the laptop. Any equipment where personal data is likely to be stored must be encrypted

- Equipment must be kept physically secure in accordance with this policy to be covered for insurance purposes. When travelling by car, best practice is to place the laptop in the boot of your car before starting your journey
- Synchronise all locally stored data, including diary entries, with the central Academy network server on a frequent basis
- Ensure portable and mobile ICT equipment is made available as necessary for anti-virus updates and software installations, patches or upgrades
- The installation of any applications or software packages must be authorised by the ICT support team, fully licensed and only carried out by your ICT support
- In areas where there are likely to be members of the general public, portable or mobile ICT equipment must not be left unattended and, wherever possible, must be kept out of sight
- Portable equipment must be transported in its protective case if supplied.

Mobile Technologies

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Mobile technologies such as Smartphones, tablets, iPads and games players are generally very familiar to children outside of the Academy. Emerging technologies will be examined for educational benefit and the risk assessed before use in the Academy is allowed. Our Academy chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

Personal Mobile Devices (including phones)

- The Academy allows staff to bring in personal mobile phones and devices for their own use. Under no circumstances does the Academy allow a member of staff to contact a pupil or parent/carer using their personal device.
- Students are allowed to bring personal mobile devices/phones to the Academy but must not use them whilst on the premises. At all times the device must be switched onto silent
- The Academy is not responsible for the loss, damage or theft of any personal mobile device
- The sending of inappropriate text messages between any member of the Academy community is not allowed
- Permission must be sought before any image or sound recordings are made on these devices of any member of the Academy community
- Users bringing personal devices into the Academy must ensure there is no inappropriate or illegal content on the device

Academy Provided Mobile Devices (including phones)

- The sending of inappropriate text messages between any member of the Academy community is not allowed
- Permission must be sought before any image or sound recordings are made on the devices of any member of the Academy community
- Where the Academy provides mobile technologies such as phones, laptops and iPads for offsite visits and trips, only these devices should be used
- Where the Academy provides a laptop for staff, only this device may be used to

conduct Academy business outside of the Academy
- Never use a hand-held mobile phone whilst driving a vehicle

Social Media, including Facebook and Twitter.

Facebook, Twitter and other forms of social media are increasingly becoming an important part of our daily lives.

- Our Academy uses Facebook and Twitter to communicate with parents and carers. The Head Teacher is responsible for all postings on these technologies and monitors responses from others
- Staff ***are not*** permitted to access their personal social media accounts using Academy equipment at ***any time during their contracted working hours***
- Students are not permitted to access their social media accounts whilst at the Academy
- Staff, governors, students, parents and carers are regularly provided with information on how to use social media responsibly and what to do if they are aware of inappropriate use by others
- Staff, governors, students, parents and carers are aware that the information, comments, images and video they post online can be viewed by others, copied and stay online forever
- Staff, governors, students, parents and carers are aware that their online behaviour should at all times be compatible with UK law

Use of Social Networking Sites for Staff

In this section ‘staff’ means employees, volunteers (including governors), agency staff, or anyone working within the school and using the schools ICT equipment.

Personal conduct

The Academy respects its staff's right to a private life. However, the school must also ensure that confidentiality with regards to its students, employees, volunteers, and its reputation are protected. It therefore requires staff using social networking websites to:

- Use caution and act responsibly when posting information on social networking sites and blogs
- Refrain from identifying themselves as working for or in any other way connected to the school
- Ensure that they do not conduct themselves in a way that conflicts with their professional code of conduct, or is otherwise detrimental to the school
- Take care not to allow their interaction on these websites to damage working relationships between members of staff, pupils at the school and their families, and other stakeholders or working partners of the Academy

If staff become aware of inappropriate material/comments they should notify the Head

Teacher as soon as possible, and if possible provide print outs of the comments made or of the pictures displayed.

Staff must not be ‘friends’ or communicate with, students on any social network sites or similar websites, including, but not limited to, ‘Facebook’, ‘Snapchat’, ‘Twitter’ etc. If any student makes contact with any staff member, they must notify the Head Teacher as soon as possible without making a response. Similarly, if any member of staff or individual associated with the school makes unintended contact with a pupil, it must be notified to the Head Teacher as soon as possible. In the absence of the Head Teacher, the Deputy or Assistant Head or a member of the SLT must be contacted. The Head Teacher can then deal with the situation as appropriate.

Staff are reminded that bullying and harassment against any other member of staff via social media sites is taken as seriously as workplace bullying and harassment. Any allegations will be dealt with under the Academy’s normal bullying and harassment or disciplinary policies, as appropriate and may also be treated as a criminal offence.

Employees that post defamatory statements that are published on the internet may be legally liable for any damage to the reputation of the individual concerned. As a representative of the Academy, any statement made by employees could mean the school is vicariously liable for those statements if done in the course of employment, even if performed without the consent or approval of the Academy. The Academy takes these acts seriously and disciplinary procedures will be invoked if any such defamatory statements are made by its employees, which may lead to dismissal.

In the case of Governors, whilst volunteers are not subject to disciplinary procedures, referral to Governor Services in the Local Authority will be made and their advice and guidance will be taken.

Appendix 1

Current legislation

Acts Relating to Monitoring of Staff Email

Data Protection Act 2018

The Act requires anyone who handles personal information to comply with important data protection principles when treating personal data relating to any living individual. The Act grants individuals rights of access to their personal data, compensation and prevention of processing.

https://www.gov.uk/data-protection

The Telecommunications (Lawful Business Practice)

(Interception of Communications) Regulations 2018

http://www.legislation.gov.uk/uksi/2018/1189/made

Regulation of Investigatory Powers Act 2000

Regulating the interception of communications and making it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998. The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, however, permit a degree of monitoring and record keeping, for example, to ensure communications are relevant to Academy activity or to investigate or detect unauthorised use of the network. Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored. Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation.

http://www.hmso.gov.uk/acts/acts2000/20000023.htm

Human Rights Act 1998

http://www.hmso.gov.uk/acts/acts1998/19980042.htm

Other Acts Relating to On-line Safety

Racial and Religious Hatred Act 2006

It a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Sexual Offences Act 2003

The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. Academies should already have a copy of "*Children & Families: Safer from*

Sexual Crime" document as part of their child protection packs.

Communications Act 2003 (section 127)

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

The Computer Misuse Act 1990 (sections 1 – 3)

Regardless of an individual's motivation, the Act makes it a criminal offence to gain:

- access to computer files or software without permission (for example using another person's password to access files)
- unauthorised access, as above, in order to commit a further criminal act (such as fraud)
- impair the operation of a computer or program

UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

Malicious Communications Act 1988 (section 1)

This legislation makes it a criminal offence to send an electronic message (email) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.

Copyright, Design and Patents Act 1988

Copyright is the right to prevent others from copying or using work without permission. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer. Copyright infringement is to copy all or a substantial part of anyone's work without obtaining the author's permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else's material. It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.

Public Order Act 1986 (sections 17 – 29)

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

Protection of Children Act 1978 (Section 1)

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is a anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

Obscene Publications Act 1959 and 1964

Publishing an “obscene” article is a criminal offence. Publishing includes electronic transmission.

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other.

A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other to fear on each of those occasions.

Acts Relating to the Protection of Personal Data

Data Protection Act 2018

The Act requires anyone who handles personal information to comply with important data protection principles when treating personal data relating to any living individual. The Act grants individuals rights of access to their personal data, compensation and prevention of processing.

https://www.gov.uk/data-protection

The Freedom of Information Act 2000

https://ico.org.uk/for-organisations/guide-to-freedom-of-information/

Appendix 2

Acceptable Use Agreement: Students

- I will only use ICT systems in Academy, including the internet, email, digital video, and mobile technologies for Academy purposes
- I will not download or install software on Academy technologies
- I will only log on to the Academy network, other systems and resources with my own user name and password
- I will follow the Academy's ICT security system and not reveal my passwords to anyone and change them regularly.
- I will only use my Academy e-mail address
- 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 a Academy project approved by my teacher
- I am aware that when I take images of students and/or staff that I must only store and use these for Academy purposes in line with Academy policy and must never distribute these outside the Academy network without the permission of all parties involved. This includes Academy breaks and all occasions when I am in Academy uniform or when otherwise representing the Academy
- I will ensure that my online activity, both in the Academy and outside Academy, will not cause my Academy, the staff, students or others distress or bring the Academy community into disrepute, including through uploads of images, video, sounds or texts
- I will support the Academy approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the Academy community
- 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 may be contacted

Appendix 3 – Letter to Parents

Dear Parent/ Carer

ICT including the internet, email, mobile technologies and online resources has become an important part of learning in our Academy. We expect all students to be safe and responsible when using any ICT. It is essential that students are aware of On-line Safety and know how to stay safe when using any ICT.

Students are expected to read and discuss this agreement with their parent/carer and then to sign and follow the terms of the agreement. Any concerns or explanation can be discussed with the On-line Safety co-ordinator, Mr Ruffell.

Please return the bottom section of this form which will be kept on record at the Academy.

✂- -

Parent/ carer signature

We have discussed this document with……………………………………………..(child's name) and we agree to follow the On-line Safety rules and to support the safe use of ICT at Sybil Andrews Academy.

Parent/ Carer Signature …….…………………..…………………………….

Student Signature……………………………………………………………………..

Tutor Group ………………………………… Date ………………………………

Appendix 4

Staff, Governor and Visitor
Acceptable Use Agreement / Code of Conduct

ICT (including data) and the related technologies such as e-mail, the internet and mobile devices are an expected part of our daily working life in the Academy. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the On-line Safety coordinator, Sarah Fisher.

- I will only use the Academy's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed acceptable by the Head Teacher and Governing Body
- I will comply with the ICT 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, personal email address, personal Twitter account, or any other social media link, 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 MIS software) 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 Teacher or Governing Body. Personal or sensitive data taken off site must be encrypted, e.g. on a password secured laptop or memory stick
- I will not install any hardware or software without permission of the On-line Safety coordinator, Sarah Fisher.
- 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 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 Head Teacher
- I will support the Academy approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the Academy community
- 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 Head Teacher
- I will respect copyright and intellectual property rights
- I will ensure that my online activity, both in the Academy and outside the Academy, will not bring the Academy, my professional role or that of others into disrepute
- I will support and promote the Academy's On-line Safety and Data Security policy and help students to be safe and responsible in their use of ICT and related technologies

User Signature

I agree to follow this code of conduct and to support the safe and secure use of ICT throughout the Academy

Signature …….…….…… Date ……

Full Name …….....(printed)

Job title ……

Appendix 5

Sybil Andrews Academy On-line Safety Incident Log

Details of ALL On-line Safety incidents to be recorded by the On-line Safety co-ordinator. This incident log will be monitored termly by the Head Teacher, Member of SLT or Chair of Governors. Any incidents involving Cyberbullying will also be recorded elsewhere

Date & time	Name of student or staff member	Male or Female	Room and computer/ device number	Details of incident (including evidence)	Actions and reasons

Appendix 6

Social Media and Criminal Offences

British Parliament's Communications Committee has defined four Social media and criminal offences -:

- **Cyber bullying**—bullying conducted using the social media or other electronic means;
- **Revenge porn**—usually following the breakup of a couple, the electronic publication or distribution of sexually explicit material (principally images) of one or both of the couple, the material having originally been provided consensually for private use;
- **Trolling**—intentional disruption of an online forum, by causing offence or starting an argument; and
- **Virtual mobbing**—whereby a number of individuals use social media or messaging to make comments to or about another individual, usually because they are opposed to that person's opinions.

The Academy will take all complaints of social media and criminal offences very seriously. All will be dealt with swiftly and where necessary the police will be involved. (See Advice for Students and Parent)

Sanctions

Violation of E-Safety rules will result in sanctions being applied to students or staff involved.

Sanctions will be set dependent on the nature of the offence. The following are guidelines – each case being judged dependent on the type of infringements, the frequency and the status of the person/s involved.

How will infringements be handled?

Whenever a student or staff member infringes the E-Safety Policy, the final decision on the level of sanction will be at the discretion of the school management.

The following are provided as exemplification only:

Students

Category A infringements

- Use of non-educational sites during lessons
- Unauthorised use of email
- Use of unauthorised instant messaging / social networking sites

[Possible Sanctions: ***referred to class teacher / tutor*** */ senior manager / E-Safety Coordinator]*

Category B infringements

- Continued use of non-educational sites during lessons after being warned
- Continued unauthorised use of email after being warned
- Continued use of unauthorised instant messaging / chatrooms, social networking sites, newsgroups
- Use of filesharing software e.g. Napster, Vanbasco, BitTorrent, LiveWire, etc
- Accidentally corrupting or destroying others' data without notifying a member of staff of it
- Accidentally accessing offensive material and not logging off or notifying a member of staff of it

[Possible Sanctions: ***referred to Class teacher/ Head of Department / Head of House / E-Safety Coordinator*** */ removal of internet access rights for a period]*

Category C infringements

- Deliberately corrupting or destroying someone's data, violating privacy of others
- Sending an email or MSN message that is regarded as harassment or of a bullying nature (one-off)
- Deliberately trying to access offensive or pornographic material
- Any purchasing or ordering of items over the internet
- Transmission of commercial or advertising material

[Possible Sanctions: ***referred to Class teacher / Head of House / E-Safety Coordinator / Head of School / removal of Internet and/or Learning Platform access rights for a period /*** *contact with parents/carers / removal of equipment]*

Other safeguarding actions

If inappropriate web material is accessed:

1. Ensure appropriate technical support filters the site
2. Inform E2BN as appropriate

Category D infringements

- Continued sending of emails or MSN messages regarded as harassment or of a bullying nature after being warned
- Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent
- Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988
- Bringing the school name into disrepute

*[Possible Sanctions – **Referred to Head of School / Contact with parents/carers** / possible exclusion / removal of equipment / refer to Community Police Officer / LA E-Safety officer]*

Other safeguarding actions:

1. Secure and preserve any evidence
2. Inform the sender's e-mail service provider

Staff

Category A infringements (Misconduct)

- Excessive use of internet for personal activities not related to professional development e.g. online shopping, personal email, instant messaging etc.
- Misuse of first level data security, e.g. wrongful use of passwords
- Breaching copyright or license e.g. installing unlicensed software on network

*[Sanction - **Referred to line manager / Head of School**. Warning given.]*

Category B infringements (Gross Misconduct)

- Serious misuse of, or deliberate damage to, any school / Council computer hardware or software;
- Any deliberate attempt to breach data protection or computer security rules;
- Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent;
- Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988;
- Bringing the school name into disrepute.

*[Sanction – **Referred to Head of School / Governors and follow school disciplinary procedures;** report to LA Personnel/ Human resources, report to Police]*

Other safeguarding actions:

- Remove the PC to a secure place to ensure that there is no further access to the PC or laptop.
- Instigate an audit of all ICT equipment by an outside agency, such as the schools ICT managed service providers - to ensure there is no risk of students accessing inappropriate materials in the school.

- Identify the precise details of the material.

If a member of staff commits an exceptionally serious act of gross misconduct they should be instantly suspended. Normally though, there will be an investigation before disciplinary action is taken for any alleged offence. As part of that the member of staff will be asked to explain their actions and these will be considered before any disciplinary action is taken.

Schools are likely to involve external support agencies as part of these investigations e.g. an ICT technical support service to investigate equipment and data evidence, the Local Authority Human Resources team.

Child Pornography found?

In the case of Child Pornography being found, the member of staff should be **immediately suspended** and the Police should be called.

Anyone may report any inappropriate or potentially illegal activity or abuse with or towards a child online to the Child Exploitation and Online Protection (CEOP):

http://www.ceop.gov.uk/reporting_abuse.html