SAMUEL WHITBREAD ACADEMY

E-Safety Policy

AUTHOR:	Principal & Head of IT Infrastructure
LOCATION:	Intranet
ACCESSIBILITY STATUS:	All staff
RELEVANT GOVERNORS COMMITTEE:	Local Governing Board

DATE OF ORIGIN:	April 2021
SENIOR TEAM REVIEW DATE:	May 2021
GOVERNOR REVIEW DATE:	May 2021
EFFECTIVE DATE:	May 2021
NEXT POLICY REVIEW DATE:	April 2022

Contents

Rationale and Aim

The purpose of this policy is to establish safe working practices in school for using IT resources, so that we get the best possible outcomes for our young people.
IT resources are a very important part of school life and provide many helpful ways to improve the outcomes for children and young people and they are a useful tool for staff to make them more effective in their work. We recognise that there are number of risks associated with using IT resources which we need to help our young people understand and protect them from. We also need to protect staff from the dangers associated with IT resources.

Policy

This policy applies to all members of the school community (including all employees, students, volunteers, parents/carers and visitors) who have access to and are users of school IT systems, both in and out of school.

Governors are responsible for the approval of the e-safety policy and for reviewing the effectiveness of the policy. A member of the Governing Body will take on the role of E-Safety Governor. The E-Safety Governor will meet with the SLT member with responsibility for IT strategy and monitor of e-safety incident logs.

The Principal and the SLT are responsible for ensuring:

- The establishment and review of the school e-safety policies and documents.
- That there is one member of the SLT team who has strategic oversight of IT. That member will be part of the safeguarding team.
- That adequate training is provided, including informing all users of the relevant procedure in the event of an e-safety allegation.
- That effective monitoring systems are set up.
- The school's Designated Senior teacher for Child Protection, and other members of the safeguarding team should be trained in e-safety issues and be aware of the potential for serious child protection issues that might arise through the use of IT.

The IT Network Manager is responsible for ensuring that:

- The school's IT infrastructure is secure and meets e-safety technical requirements.
- The school's password policy is adhered to.
- The school's filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person.
- They keep up to date with e-safety technical information.
- The use of the school's IT infrastructure is regularly monitored in order that any misuse or attempted misuse can be reported to the appropriate persons.

Note, currently Samuel Whitbread Academy (SWA) engages the services of Partnership Education for day-to-day support of the school's PCs, laptops, printers and servers with BEST IT Support Team providing authority infrastructure. The IT Manager therefore has an additional responsibility to ensure that the support team adhere to the above e-safety measures during the course of their activities and are aware of the Security and Acceptable Usage Policy.

Teachers and Support staff are responsible for ensuring that:

- They have an up to date awareness of e-safety matters and of the current school e-safety policy and practices.
- They have read, understood and signed the school Staff Acceptable Usage Policy (appendix 2).
- E-safety issues are embedded in the curriculum and other school activities.
- Students understand and follow the school's e-safety and acceptable usage policies.
- Students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- They monitor IT activity in lessons, extracurricular and extended school activities, including the appropriateness of websites for research etc.
- Reporting abuse, misuse or notifying of access to inappropriate materials.

Students are responsible for ensuring that:

- Using the school IT systems in accordance with the Student (appendix 1) Acceptable Usage Policy, which will also be shared with parents/carers.
- Reporting abuse, misuse or notifying of access to inappropriate materials.
- Adopting good e-safety practice when using digital technologies out of school and realise that the school's e-safety policy also covers their actions out of school, if related to their membership of the school.
- They have read, understood and signed the school Student Acceptable Usage Policy (appendix 1)

Procedure

This policy should be read in conjunction with the BEST Data Protection Policy[1]

Email

All digital communications with students should be on a professional level and only carried out using official school systems (see staff guidance in child protection policy).

Under no circumstances should staff contact pupils, parents/carers or conduct any school business using personal e-mail addresses.

School e-mail is not to be used for personal use.

Staff should be mindful of the need to protect other users', such as parents', personal email addresses when sending emails to more than one address by using the Blind Carbon Copy (Bcc) option in an email client.

Mobile Devices and digital images.

When taking students off site, only the school mobile phone ("the trip phone") should be used to phone parents/carers/students.

Staff should avoid, wherever possible, using their own personal devices to record digital images (photos or videos) of students, rather they should be using school owned mobile devices. Where this is not practical, the images should be transferred

[1] https://www.bestacademies.org.uk/legal/

to the school network shared drives, including SWA cloud storage (Google Drive), or to an official school social media account (such as a department twitter account) and then the original photos should be removed from the private phone, and any personal backups deleted. Staff should not store images or videos of students on their own personal devices.

Staff will not post images of children from other schools on SWA social media (for example in sports fixtures).
The school record of parental permissions granted/not granted must be adhered to when taking images of our students. A list will be circulated by the data office and referred to by staff when taking photos of students. It is best practice when posting an image of a child to not associate their name with the photo.
In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other students / pupils in the digital / video images.

Social Networking Sites

Young people will not be allowed on social networking sites from school equipment. Filtering solutions will be in place to not give access to those sites.
Staff users will follow the expectations set out in our HR and Safeguarding policies regarding use of social media. Only official department twitter accounts should be used to communicate news and events with parents and students. The administration of a department twitter account must be shared within a department team for the sake of open-ness and transparency.
Staff users should not reveal names of staff, pupils, parents/carers or any other member of the school community online on any personal social networking site**.**
Students/parents/carers should be aware the school will investigate misuse of social networking if it impacts on the well-being of other students or stakeholders.

If inappropriate comments are placed on social networking sites about the school or school staff then advice would be sought from the relevant agencies, including the police if necessary.
The school will endeavour whenever possible to use social networking in positive ways to publicise, inform and communicate information.

Data Security: Files and Cloud storage

Staff are expected to use Google Drives for storage of all files and folders. Shared drives for departments and multiuser use are created to enable sharing and collaboration of data.

The use of USB storage devices are discouraged as this can lead to the unintentional threat of malware and other IT security issues. When accessing and storing folders staff should always keep in mind GDPR best practice and refer to the SWA GDPR policy where appropriate.

Security: Virus and other Malware

Staff should be always conscious when accessing emails and files that could be a security threat. Consider the following:

- Do you know who sent the email?
- Is the email structure correct when you look at the properties of the address?
- Is the content relevant?
- Delete junk emails without opening.
- Do not open suspicious hyperlinks in emails.
- Do not open suspicious attachments.

Network monitoring

The school uses internet monitoring software for students. This includes private devices when connected to our network.
The school only allows the IT Manager, Safeguarding Team and SLT to access Internet logs.

Passwords

Staff

Passwords or encryption keys should not be recorded on paper or in an unprotected file. Passwords should be changed in line with best practice guidance, as advised by the network manager.

Students

Should only let school staff know their in-school passwords. Inform staff immediately if passwords are traced or forgotten. All staff are able to access the network to allow students to change passwords.

Use of Own Equipment

Students are encouraged to bring their own devices to school (BYOD), but must follow the instructions of teachers in relation to their use in school. All private equipment is brought in to school at the owners' risk and the school takes no responsibility for loss or damage to that equipment whilst it is on site.

Use of School Equipment

No personally owned applications or software packages should be installed on to school IT equipment.

Personal or sensitive data (belonging to staff) should not be stored on the local drives of desktop or laptop PCs. If it is necessary to do so, the local drive must be encrypted.

All users should ensure any screens are locked (by pressing Ctrl, Alt, Del simultaneously) before moving away from a computer during the normal working day to protect any personal, sensitive, confidential or classified data and to prevent unauthorised access.

Responding to incidents of misuse

Any e-safety incidents must immediately be reported to the SLT member with strategic oversight of IT who will investigate further.

Staff investigating an incident should immediately impound the equipment if needed.

There may be times when infringements of the policy could take place through careless, irresponsible or deliberate misuse.

If any apparent or actual, misuse appears to involve illegal activity e.g. child sexual abuse images, adult material which potentially breaches the Obscene Publications Act, criminally racist material or other criminal conduct, activity or materials then advice should be sought from relevant authorities.

If it is suspected that misuse might have taken place, but that the misuse is not illegal (as above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. It is recommended that more than one member of staff is involved in the investigation which should be carried out on a "clean" designated computer. It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. This will be done in line with HR and safeguarding policies.

<u>Sexting</u> (Reference to UK Council for Child Internet Safety (UKCCIS))

The Law

Making, possessing, and distributing any imagery of someone under 18 which is indecent is illegal. This includes imagery of yourself if you're under 18.

Indecent is not definitively defined in law, but images are likely to be considered indecent if they depict:

- a naked young person
- a topless girl
- an image which displays genitals, and
- sex acts including masturbation.
- indecent images may also include overtly sexual images of young people in their underwear

These laws weren't created to criminalise young people but to protect them. Although sharing sexual images of themselves is illegal and risky, it is often the result of curiosity and exploration. Young people need education, support, and safeguarding, not criminalisation. We hold the same view as the National Police

Chiefs' Council (NPCC), that it is clear that "youth-produced sexual imagery should be primarily treated as a safeguarding issue." We will look to support our students that choose to undertake this risky activity with assemblies, tutor time activities and outside agency referrals where appropriate. SWA will try, where possible to resolve such issues without involving the police. However, in some circumstances, the police must always be involved.

Handling incidents

- Refer to the Designated Safeguarding Lead (DSL)
- DSL or member of safeguarding team will meet with the young people involved
- SWA staff will not view the image unless it is unavoidable
- SWA safeguarding staff will take every step to discuss with parents
- Any concern the young person is at risk of harm, contact social care or the police

SWA staff will always refer to the police or social care if incident involves:

- an adult
- coercion, blackmail, or grooming
- concerns about capacity to consent, [e.g., SEN]
- images show atypical sexual behaviour for the child's developmental stage
- violent acts are depicted
- image shows sex acts and includes a child under 13
- a young person at risk of immediate harm as a result of the disclosure (for example, self-harm or suicide)

Viewing images

- Staff should avoid viewing youth-produced sexual imagery. Instead, respond to what you have been told the image contains.
- If it is felt necessary to view, discuss with the Principal or DSL first.
- Staff should never copy, print, or share the image (it's illegal).
- If it is felt necessary to view the image members of the safe guarding team should view with another member of safeguarding team present.
- Staff will record the fact that the images were viewed along with reasons and who was present. The record will be signed and dated.

Deleting images (from devices and social media)

If the DSL has decided that involving other agencies is not necessary, consideration should be given to deleting the images.
Pupils will be asked to delete the images themselves and confirm they have done so. This should be recorded, signed, and dated on the sexting referral form.
Any refusal to delete the images should be treated seriously, reminding the pupil that possession is unlawful. Parents will be informed.

Links with other Policies

This policy must also be read in conjunction with the behaviour, safeguarding, HR, anti-bullying policies and the BEST Data Protection policy and is in line with KCSIE and safer working practice (both 2019).

Monitoring and Evaluation

All incidents of IT misuse are logged. Trends are analysed and appropriate action taken by senior staff.

Implementation and Review

This policy will be made known to all staff, parents/carers and governors, and published on the Academy website. Copies are also available upon request from the Academy office. This policy will be reviewed annually or as required.

Appendix 1 - Acceptable Use Policy – Students

You are expected to use the school network in a responsible manner. This is not a complete list of everything that is unacceptable, all use should be consistent with our school's high expectations. Irresponsible use may result in the loss of school network access, contact with parents or in the event of illegal activities, contact with the police.

- ☐ I will only access the school network through my authorised username and password. I will not use the passwords of others.
- ☐ I understand that my network use, including that on my own personal device is monitored by the school.
- ☐ I will use Google Drive for storage of my schoolwork data. The use of Google Drive enables and supports cross platform access from cloud storage and any associated security and viral protection offered from ransomware and other similar threats.
- ☐ I will only use my network drive for storage for lessons that are not able to use Google storage; this includes Music, Computer Studies, Media and Design & Engineering
- ☐ I will not disclose details of the school network and infrastructure to anyone outside of the school such as passwords, IP Addresses, Domain names and other similar configuration details. This is not an exclusive list.
- ☐ I will not create, send or post any material that is likely to cause offence or needless anxiety to other people or bring the school (or Bedfordshire Schools Trust) into disrepute.
- ☐ All illegal activities are forbidden. I will not create material that is offensive, that discriminates against groups or individuals or that incites hatred against others.
- ☐ I will not access any materials which are illegal, inappropriate or which may cause harm and distress to others.
- ☐ I will use appropriate language, remembering that I am representing the school on a global public system.
- ☐ I will not try to use any programmes or software that might allow me to bypass the filtering and security systems in place, such as VPNs on my own devices on the school network.

☐ I will not try to install programmes on any school computer or try to alter computer settings.

☐ I will only use my personal devices in school at times that are permitted.

☐ I will not open emails unless I know and trust the person/organisation who has sent them.

☐ For my own safety and that of others, I will not disclose personal information about myself or others when on-line. I will not arrange to meet 'on-line friends' unless I take an adult.

☐ I will not take, or distribute, images of anyone without their permission.

☐ I will only use social networking sites with permission and at the times that are allowed.

☐ I will report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

☐ Where the material I research on the Internet is protected by copyright, I will not download copies, including music and video. I will only use the work of others found on the Internet in my own work with their permission.

☐ I will immediately report any damage or faults involving IT equipment, however this may have happened.

I have read and understand the above and agree to use the SWA IT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Signed: …….

Name: …….

Date: …….

Appendix 2 - Acceptable Use Policy – Staff and Volunteers

You are expected to use the school network in a professional manner. This is not a complete list of everything that is unacceptable, all use should be consistent with our school's high expectations.

- ☐ I understand that I must use SWA IT systems in a responsible way to ensure that there is no risk to my safety or to the safety and security of the IT systems and other users.
- ☐ I understand that the school will monitor my use of IT systems, email and other digital communications, including on my personal device when connected to the school's network.
- ☐ I understand the rules set out in this agreement also apply to the use of the school IT systems (e.g. laptops, email) out of the school.
- ☐ I understand that the school IT systems are primarily intended for educational use and that I will only use systems for personal or recreational use within the policies and rules set down by the school.
- ☐ I will not disclose my username and password to anyone else, nor will I try to use any other person's username and password.
- ☐ I will immediately report any illegal, inappropriate or harmful material/incident I become aware of to the appropriate person.
- ☐ I will communicate with others in a professional manner. I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- ☐ I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital/video images. If I have used my personal device for this, I will transfer them to the school network, or a department twitter account as soon as possible and delete all copies from my device and any backups.
- ☐ In line with HR and Safeguarding policies I will use social media appropriately. I will not make contact with any students on private, closed social media platforms.
- ☐ I will only communicate with students and parents/carers using official school systems. Any such communication will be professional in tone and manner.

- ☐ I will not engage in any on-line activity that may compromise my professional responsibilities, or bring the School or the Trust into disrepute.
- ☐ When I use my personal mobile devices in the school, I will follow the rules set out in this agreement, in the same way as if I was using school's equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses and that any sensitive information is encrypted and password protected.
- ☐ I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- ☐ I will not access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- ☐ I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.
- ☐ I will use Google Drive for storage of all school related data. The use of Google Drive enables and supports cross platform access from cloud storage and any associated security and viral protection offered from ransomware and other similar threats.
- ☐ I will only use my network drive for storage for lessons that are not able to use Google storage; this includes Music, Computer Studies, Media and Design & Engineering
- ☐ I will not disclose details of the school network and infrastructure to anyone outside of the school such as passwords, IP Addresses, Domain names and other similar configuration details. This is not an exclusive list.
- ☐ I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- ☐ Where personal data is transferred outside the secure network, it must be encrypted.

☐ I understand that data protection policy requires that any staff or learner data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by policy to disclose such information to an appropriate authority.

☐ I will immediately report any damage or faults involving equipment or software.

☐ Where work is protected by copyright, I will not download or distribute copies (including music and videos).

☐ I understand that this Acceptable Use Policy applies not only to my work and use of SWA IT equipment in school, but also applies to my use of school IT systems and equipment out of the school and my use of personal equipment in the school or in situations related to my employment by SWA.

☐ I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action.

I have read and understand the above and agree to use the SWA IT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff/Volunteer

Name: ……..

Signed: …….

Date: ……...