Saint Martin's

Acceptable Use Policy

.

Authors	**Matthew Connor-Hemming**
Version	**1**
Description of changes	**New policy**
Date of Approval	**November 2018**
Review Date	**November 2019**

Scope of this Policy

This policy applies to all members of the school community, including staff, pupils, parents, and visitors. In this policy 'staff' includes teaching and non-teaching staff, governors, and regular volunteers (but access to systems is not intended in any way to imply an employment relationship). 'Parents' include, where applicable, pupils' carers and those with parental responsibility. 'Visitors' includes anyone else who comes to the school, including occasional volunteers.

Interaction with other policies

There is a clear overlap in this area between staff and pupil conduct, data security, child protection, personal privacy online, and good practice including around digital record keeping (including both email use and retention). This means that the Acceptable Use Policy does not stand on its own but must sit alongside related policies (applicable to staff or pupils), including where applicable:

(a) Privacy Notices (those aimed at pupils / parent and staff);
(b) Child Protection Policy;
(c) Staff Code of Conduct;
(d) Staff Data Protection Policy;
(e) Anti bullying Policy;
(f) Whistleblowing Policy;
(g) e-Safety Policy;
(h) Taking, Storing and Using Images of Children Policy;
(i) Data Breach Policy; and
(j) Data Retention Policy.

Relevant background

This policy and note is written having had regard to the following guidance and regulation:

- *Keeping Children Safe in Education (KCSIE)* (September 2018)
- *Working Together to Safeguard Children* (2018)
- *Independent Schools Standards Regulations*
- *Prevent Duty Guidance for England and Wales* (Revised July 2015)
- *The use of social media for online radicalisation* (July 2015)

Online behaviour

As a member of the school community you should follow these principles in all of your online activities:

- Ensure that your online communications, and any content you share online, are respectful of others and composed in a way you would wish to stand by
- Do not access, create or share content that is illegal, deceptive, or likely to offend other members of the school community (for example, content that is obscene, or promotes violence, discrimination, or extremism, or raises safeguarding issues)

- Respect the privacy of others. Do not share photos, videos, contact details, or other information about members of the school community, even if the content is not shared publicly, without going through official channels and obtaining permission
- Do not access or share material that infringes copyright, and do not claim the work of others as your own
- Do not use the internet to distribute malicious software, to damage, interfere with, or gain unauthorised access to the computer systems of others, or carry out illegal activities
- Staff should not use their personal email, or social media accounts to contact pupils or parents, and pupils and parents should not attempt to discover or contact the personal email addresses or social media accounts of staff.

Using the school's IT systems

Whenever you use the school's IT systems (including by connecting your own device to the network) you should follow these principles:

- Only access school IT systems using your own username and password. Do not share your username or password with anyone else
- Do not attempt to circumvent the content filters or other security measures installed on the school's IT systems, and do not attempt to access parts of the system that you do not have permission to access
- Do not attempt to install software on, or otherwise alter, school IT systems
- Do not use the school's IT systems in a way that breaches the principles of online behaviour set out above
- Remember that the school monitors use of the school's IT systems, and that the school can view content accessed or sent via its systems.

Passwords

Passwords protect the School’s network and computer system and are your responsibility. They should not be obvious (for example "password", 123456, a family name or birthdays), and nor should they be the same as your widely-used personal passwords. You should not let anyone else know your password, nor keep a list of passwords where they may be accessed, and must change it immediately if it appears to be compromised. You should not attempt to gain unauthorised access to anyone else’s computer account or to confidential information to which you do not have access rights.

Use of Property

Any IT property belonging to the School should be treated with respect and care, and used only in accordance with any training and policies provided. You must report any faults or breakages without delay to the ICT department.

Use of school systems

The provision of school email accounts, Wi-Fi and internet access is for official school business, administration and education. Staff and pupils should keep their personal, family and social lives separate from their school IT use and limit as far as possible any personal use of these accounts. Again, please be aware of the school's right to monitor and access web history and email use.

Use of personal devices or accounts and working remotely

All official school business must be conducted on school systems, and it is not permissible to use personal email accounts for school business. Any use of personal devices for school purposes, and any removal of personal data or confidential information from school systems – by any means including email, printing, file transfer, cloud or (encrypted) memory stick – must be registered and approved by the ICT department.

Where permission is given for use of personal devices, these must be subject to appropriate safeguards in line with the school's policies, including encryption etc.

Monitoring and access

Staff, parents and pupils should be aware that school email and internet usage (including through school Wi-Fi) will be monitored for safeguarding, conduct and performance purposes, and both web history and school email accounts may be accessed by the school where necessary for a lawful purpose – including serious conduct or welfare concerns, extremism and the protection of others.

Any personal devices used by pupils, whether or not such use is permitted, may be confiscated and examined under such circumstances. The school may require staff to conduct searches of pupil’s personal accounts or devices if they were used for school business in contravention of this policy.

Compliance with related school policies

You will ensure that you comply with the school's e-Safety Policy and Privacy Notices, Child Protection Policy, Staff Code of Conduct, Staff Data Protection Policy, Anti bullying Policy, Whistleblowing Policy, Taking, Storing and Using Images of Children Policy, Data Breach Policy, and the Data Retention Policy.

Retention of digital data

Staff and pupils must be aware that all emails sent or received on school systems will be kept in archive whilst they are still at School and email accounts will be closed and the contents deleted within 90 days of that person leaving the school. Important information that is necessary to be kept should be held on the relevant personnel or pupil file, not kept in personal folders, archives or inboxes. Hence it is the responsibility of each account user to ensure that important information is retained in the right place or, where applicable, provided to the right colleague. That way no important information should ever be lost as a result of the school's email deletion protocol.

If you consider that reasons exist for the protocol not to apply, or need assistance in how to retain and appropriately archive data, please contact **PCO@saintmartins-school.com**.

Breach reporting

The law requires the school to notify personal data breaches, if they are likely to cause harm, to the authorities and, in some cases, to those affected. A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

This will include almost any loss of, or compromise to, personal data held by the school regardless of whether the personal data falls into a third party's hands. This would include:

- loss of an unencrypted laptop, USB stick or a physical file containing personal data;
- any external hacking of the school's systems, eg through the use of malware;
- application of the wrong privacy settings to online systems;
- misdirected post, fax or email;
- failing to bcc recipients of a mass email; and
- unsecure disposal.

The school must generally report personal data breaches to the Information Commissioner's Office (ICO) without undue delay (ie within 72 hours), and certainly if it presents a risk to individuals. In addition, controllers must notify individuals affected if that risk is high. In any event, the school must keep a record of any personal data breaches, regardless of whether we need to notify the ICO.

If staff become aware of a suspected breach, they should refer to the School's Data Breach Policy. If pupils become aware of a suspected breach, they should refer to their form tutor.

Data breaches will happen to all organisations, but the school must take steps to ensure they are as rare and limited as possible and that, when they do happen, the worst effects are contained and mitigated. This requires the involvement and support of all staff and pupils. The school's primary interest and responsibility is in protecting potential victims and having visibility of how effective its policies and training are. Accordingly, falling victim to a data breach, either by human error or malicious attack, will not always be the result of a serious conduct issue or breach of policy; but failure to report a breach will be a disciplinary offence.

Breaches of this policy

A deliberate breach of this policy will be dealt with as a disciplinary matter using the school's usual procedures. In addition, a deliberate breach may result in the school restricting your access to school IT systems.

If you become aware of a breach of this policy or the e-Safety Policy, or you are concerned that a member of the school community is being harassed or harmed online you should report it to the DSL. Reports will be treated in confidence.

Acceptance of this policy – staff

Please confirm that you understand and accept this policy by signing below and returning the signed copy to the HR Manager.

I understand and accept this acceptable use policy

Name: …………………………………………………………

Signature: …………………………………………………………

Date: …………………………………………………………

Acceptance of this policy - pupils

Each pupil will be expected to confirm that they understand and accept this policy by signing the Acceptable Use Agreement (AUA) relevant to their age. This will be done in form time. It will be done annually.

The pupils will be asked to take the AUA with a copy of this Policy and discuss it with their parents/carers who must sign the AUA. The signed AUA must be returned to the form tutor. The AUAs are attached at Appendix 1.

Saint Martin's

Appendix 1

Acceptable Use Agreement – Senior School and Sixth Form

Saint Martin's school promotes the use of technology in school as all pupils will need the skills and knowledge in whatever field of work they enter when they become an adult. We ensure that our school IT network is robust and resilient and we do our upmost to ensure the safety of children when using it. It is important that pupils abide by the school rules when using technology in school and inform a member of staff immediately, if they become aware of any misuse.

This Agreement highlights the do's/don'ts of using all technology in school and shows how we want pupils to behave when using IT. Any misuse will result in pupils being temporarily banned from using the school network. In addition, the AUA covers the following legislation:

- Malicious Communications Act
- GDPR 2018
- Computer Misuse Act 1990
- Communications Act 2003
- Sexual Offences Act 2003

Please read carefully and sign at the bottom to show you agree to these terms. If you do not sign and return this form you will not be able to use the IT systems in school.

<u>For Pupils</u>

<u>Using Technology in Schools</u>

- I will only use school Internet, IT facilities and mobile technologies for educational purposes which follow the teachers' instructions. This includes email, video, messaging, video-conferencing, using software apps, social media, Internet, file-saving and printing.
- I will only use my mobile phone, mobile device or smartwatch in school when permission has been granted by a teacher. If permission is granted, I will use my mobile device in line with how I would use other technology in school.
- I will not look at or delete or amend other people's work or files.
- I will treat all IT equipment at school with respect and ensure the computer or mobile device is left in the state that I found it.

<u>Security, Passwords & Copyright</u>

- I will not install software on school IT facilities due to the risk of damage being caused by malware or viruses. I will ask an ICT teacher or technician to install software if required.
- I will only install software apps on mobile devices when directed to by a teacher. I will only use school-related information when registering for an app.
- I will not share my network, Internet or any other school-related passwords.
- I will change my passwords when asked to and ensure that they have complexity e.g. Capital, lower case letters, numbers and symbols.
- I will only use my school-supplied email address for school-related activities.
- I will respect copyright when making use of images, videos or other media in my

school work. I will use and attribute 'Creative Commons' material as taught in ICT/e-safety lessons.

- I will follow the school procedures when using removable media e.g. flash drives to ensure that I don't infect any machines.
- I will not look for ways to bypass the school filtering, monitoring or proxy service.
- I will not bypass the school filtering, monitoring or proxy service.

Online Behaviour & Safety

- I will make sure all my contact with other people at school is responsible. I will not cyber bully pupils, teachers or other members of staff.
- I will be responsible and polite when I talk online to pupils, teachers and other people related to the school, both in school-time and outside school-time.
- I won't look for or look at unpleasant, unsuitable or extremist websites in school. I will check with a teacher if I think a website might be unsuitable.
- I won't give out my personal details, such as my name, address, school or phone number on the Internet.
- I won't meet people I've met on the Internet unless I have told my parents and they come with me.
- I won't upload or download any pictures, writing or films which might upset people online.
- I won't write unpleasant, rude or untrue comments online about pupils, teachers or other staff employed by the school.
- I won't share inappropriate images or videos of other pupils on the school network or personal devices.
- I am aware that everything I do on the computers at school is monitored and logged, and that the school can talk to my parents if a teacher is concerned about my online safety or my behaviour when using school computers.
- I will not look for, view, upload or download offensive, illegal, copyright-infringing or pornographic material. If I find such material on school IT equipment I will inform a teacher immediately.
- I understand that these rules are designed to keep me safe and that if they are not followed, sanctions may be applied and my parent/guardian may be contacted.

For parents:

- I agree to support and uphold the principles of this policy in relation to my child and their use of the Internet, at home and at school.
- I agree to uphold the principles of this policy in relation to my own use of the Internet, when that use is related to the school, employees of the school and other pupils at the school.
- Images of pupils will only be taken, stored and used for school purposes in line with school policy. Images will only be used on the Internet or in the media with permission.

Pupil's name…………………………………………

Pupil's signature……………………………………

Parent's name………………………………………

Parent's signature…………………………………

Date…………………………………………………

Saint Martin's

Acceptable Use Agreement: Junior School

I have read this with my teacher and with my parents at home

I will use ICT in School only for school work ☺ ☹

I will only use my own files or teacher approved files on the computer ☺ ☹

I will keep my logons and passwords private ☺ ☹

I will not give out my personal information online ☺ ☹

I will tell the teacher if I see anything that upsets me online ☺ ☹

I will not upload or send any pictures, videos, sounds or text that might upset someone. ☺ ☹

I will not wear a Smart Watch to school if it has access to the Internet ☺ ☹

I know my ICT use at school is checked ☺ ☹

I know the e-safety rules keep me safe and I will be responsible for my own behaviour ☺ ☹

I know my parents will be contacted if school is worried about my e-safety ☺ ☹

Name: ______________________________________ Date: __________________

Signed by Parent: ________________________________

Pupils' Acceptable Use Agreement : Alice House

Saint Martin's

I have read this at school with my teacher and with my parents at home.

I will use ICT in School only for school work.

☺ ☹

I will tell my teacher if I see anything that upsets me online.

☺ ☹

I will not upset anyone by taking photos/ videos/ sounds or using text.

☺ ☹

I know my parents will be contacted if school is worried about my e safety.

☺ ☹

I will only use my own files on the computer.

☺ ☹

I will not give out my name, address or phone number online.

☺ ☹

I will only tell my teacher and my parents my ICT login or password.

☺ ☹

I know my ICT use at school is checked.

☺ ☹

I will only take sensible photos on school I pads.

☺ ☹

I know the e safety rules keep me safe.

☺ ☹

Name ______________________ Date ___________

Signed by parent _____________________________