Saint Martin's

E-safety Policy

Authors	Nicola Smillie/Matthew Connor Hemming
Version	3
Description of changes	Changes for KCSIE 2018 – see table
Date of Approval	November 2018
Review Date	November 2019

Introduction

Saint Martin’s School (“the School”) recognises its duty to ensure every pupil in its care is safe in the digital world. The pupils are therefore taught how to stay safe in the online environment and how to mitigate risks, including but not limited to the risk of identity theft, bullying, harassment, grooming, stalking and abuse.

This Policy applies to all members of the School community who have access to and are users of the School ICT systems, both in and out of School.

Current and emerging technologies used in and outside of School include:

- Websites
- Apps
- Email and instant messaging
- Blogs
- Social networking sites
- Chat rooms
- Learning platforms and virtual learning environments
- Music / video downloads
- Gaming sites
- Text messaging and picture messaging
- Video Sharing
- Podcasting
- Online communities via games consoles
- Mobile internet devices such as smart phones and tablets.
- Smart watches

This policy is compliant with the latest ISI Regulatory Requirements and Keeping Children Safe in Education “KCSIE” (September 2018) and includes reference to the following documents/internet sites:

- NSPCC “On line Abuse and Bullying Prevent Guide for Professionals Working with Young People
- The use of Social Media for online radicalisation
- The UK Safer Internet Centre
- CEOP “Thinkuknow” website

This policy, supported by the Acceptable Use Policy for all staff and pupils, is implemented to protect the interests and safety of the whole School community. It aims to provide clear guidance on how to minimise risks and how to deal with any infringements. It is linked to the following School policies:

- Child Protection
- Health and Safety
- Behaviour
- Anti-Bullying
- Acceptable Use Policy
- Data Protection
- PSHCEE
- Staff Code of Conduct
- Prevent Action Plan
- Taking, Storing and Using Images of Children Policy

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly online resources, is not consistently policed. All users need to be aware of the range of risks associated with the use of these internet technologies.

The School has a duty of care to educate the pupils on e-safety issues; teaching them the appropriate behaviours and critical thinking skills necessary to enable them to remain both safe and within the law when using the internet and related technologies in and beyond the classroom.

Both this policy and the Acceptable Use Policy cover fixed and mobile internet devices provided by the School (such as PCs, laptops, webcams, tablets, whiteboards, digital video equipment, etc.); as well as all devices owned by pupils and staff brought onto School premises (personal laptops, tablets, smart phones, etc.).

Roles and responsibilities

Every member of staff has a duty of care for ensuring the safety (including e-safety) of members of the School Community although the day to day responsibility for e-safety will be delegated to the Network Manager. The Deputy Head (DSL) is the e-Safety Co-ordinator.

The e-Safety Co-ordinator should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.

The Head is responsible for ensuring that the Network Manager and e-Safety Co-ordinator, and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.

The Head will ensure that there is a system in place to allow for monitoring and support of those in School who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

The Head will be advised by the Network Manager if there are any concerns relating to electronic activity.

The Network Manager is responsible for ensuring that:

- the School’s technical infrastructure is secure and is not open to misuse or malicious attack
- the School meets required e-safety technical requirements
- users may only access the networks and devices through a properly enforced password protection policy, in which passwords are changed every term except for pupils in Alice House and Junior School
- the filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- appropriate parameters for alerts and online reports are in place in consultation with the e-Safety Co-ordinator
- providing support in designing the online reports
- the daily monitoring of alerts is in place and that these are reported to the e-Safety co-ordinator immediately
- he keeps up to date with e-safety technical information in order to effectively carry out his e-safety role and to inform and update others as relevant
- the use of the network /internet / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Head as e-Safety Coordinator for investigation / action / sanction
- monitoring software / systems are implemented and updated as agreed in School policies
- ICT equipment owned by the School is inspected regularly without notice
- Email or voicemail can be accessed in a pupil’s or staff member’s absence to deal with a business related issue.

The e-Safety Co-ordinator is responsible for:

- co-ordinating the education of pupils about e-safety matters, which is mainly delivered through ICT lessons, PSHCEE and assemblies

- keeping up to date with current e-Safety issues and guidance issued by organisations such as Solihull MBC, CEOP (Child Exploitation and Online Protections), E-Safety Support, UK Council for Child Internet Safety, The UK Safer Internet Centre and Childnet International and updating the members of staff responsible for PSHCEE delivery working closely with the Designated Safeguarding Leads (DSLs) who receive updates from the LSCB
- chairing an e-safety meeting every half term, to include the DSLs, Head of ICT, ICT Co-ordinators in Early Years Foundation Stage (EYFS), Key Stage1 and Key Stage2, Network Manager and Head of PSHCEE
- responding to misuse /attempted abuse reported by the Network Manager or a member of staff
- monitoring online reports on a weekly basis
- ensuring that they are trained in e-safety issues and aware of the potential for serious child protection issues arising from the
    - sharing of personal data
    - access to illegal/inappropriate materials
    - inappropriate online contact with adults/strangers
    - potential or actual incidents of grooming
    - cyber-bullying
- reporting to the e-Safety Governor (the Nominated Governor for Child Protection) to discuss current issues, review incident logs, reviewing filters etc.
- providing advice and training for staff

The Senior Leadership Team and the Network Manager have responsibility for ensuring this policy is upheld by all members of the School community. They will keep up to date on e-safety as with all issues of safety at this School. The School believes that it is essential for parents / carers to be fully involved with promoting e-safety both in and outside of School. Information is provided to parents and carers through letters, newsletters, blogs, reference to relevant web sites/ publications, information evenings etc and seek to promote a wide understanding of the benefits and risks related to internet usage.

The Governing Body is responsible for the approval of the e-Safety Policy and for reviewing its effectiveness. This will be carried out by receiving regular information about e-safety incidents and monitoring reports. This is included within the remit of the Governor for Child Protection whose role includes regular meetings with the e-safety coordinator, regular monitoring of e-safety logs and reporting to relevant Governors' meetings. The effectiveness of this policy forms part of the annual review carried out by the Nominated Governor.

Parental Involvement

It is essential for parents/carers to be fully involved with promoting e-Safety both in and outside of School and to be aware of their responsibilities. The School discusses e-Safety with parents/ carers and seeks to promote a wide understanding of the benefits of new technologies, together with the associated risks.

- Parents/carers and pupils are actively encouraged to contribute to reviews of the School e-Safety policy via the e-Safety Co-ordinator
- Parents/carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to the School
- 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 School website). A form is sent to the parents on a pupil's entry to school and retained on the pupil's file. A list of pupil's for whom consent has not been given is held by the marketing team with a copy on each staff noticeboard
- Parents/carers are encouraged to support the School approach to online safety and not upload or add any text, image, sound or videos that could upset or offend any member of the School community, or bring the School name into disrepute and to ensure their online activity would not cause the School, staff, pupils or others distress or bring the School community into disrepute

- Parents/carers are expected to support the School's policy and help prevent their child/children from signing up to services such as Facebook, Instagram, Snapchat and YouTube whilst they are underage (13+ years in most cases)
- The School disseminates information to parents relating to eSafety where appropriate in the form of;
- Information evenings
- Posters
- School website information
- Newsletter items
- E-safety policy (sent to parents and available on the website)

Staff awareness

New staff must sign to agree to the School's Acceptable Use Policy as part of their induction. All staff receive updates on e-safety at whole School staff meetings and other training sessions and are made aware of their individual responsibilities relating to the safeguarding of children within the context of e-safety.

All staff working with children are responsible for demonstrating, promoting and supporting safe behaviours in their classrooms and following School e-Safety procedures. These behaviours are summarised in the Acceptable Use Policy which must be signed and returned before being issued a computer account.

Teaching staff are encouraged to incorporate e-safety activities and awareness within their subject areas and through a culture of talking about issues as they arise. They should know what to do in the event of misuse of technology by any member of the School community.

A record of concern must be completed by staff as soon as possible if any incident relating to e-safety occurs and be provided directly to the School's e-Safety Coordinator and DSLs.

E-Safety in the curriculum and School community

ICT and online resources are used increasingly across the curriculum. It is essential for e-safety guidance to be given to pupils on a regular and meaningful basis. The School continually look for new opportunities to promote e-safety and regularly monitor and assess the pupils' understanding of it.

The School provides opportunities to teach about e-safety within a range of curriculum areas and ICT lessons. Educating pupils on the dangers of technologies that may be encountered outside School will also be carried out via Personal, Social, Health, Citizenship, Economic Education and Social Emotional Aspects of Learning as well as informally when opportunities arise.

From EYFS pupils are taught to look after their own online safety. From Year 6 pupils are taught about recognising online sexual exploitation, stalking and grooming, the risks, and of their duty to report any such instances they or their peers come across. Pupils can report concerns to the DSL, the e-Safety Coordinator and any member of staff at the School.

From Year 2 pupils are also taught about relevant laws applicable to using the internet; such as data protection and intellectual property. Pupils are taught about respecting other people's information and images etc through discussion and classroom activities.

Pupils should be aware of the impact of cyber-bullying and know how to seek help if they are affected by these issues (see also the School's Anti-bullying Policy). Pupils should approach a DSL, the e-Safety Coordinator as well as parents, peers and other staff for advice or help if they experience problems when using the internet and related technologies.

The School has regard to the Prevent Duty and the risk of online radicalisation. All staff receive training on Prevent and details are in the Child Protection Policy and the Prevent Risk Assessment and Action Plan.

The School’s Technical Provision and Associated Safeguards

Appropriate filters and monitoring systems are in place to safeguard children from potentially harmful and inappropriate material online. ‘Smoothwall’ is in place to provide the appropriate hardware and support services to ensure the School has a robust web-filtering and appropriate reporting capability to meet the demands of our safeguarding duties. As part of this, the Smoothwall systems produce and enable us to report on web usage. Clear daily reports of ‘suspicious activity’ are provided for the e-safety coordinator so that she can monitor web searches in line with safeguarding and ‘Prevent’ recommendations.

Girls in Years 3 – 11 are not allowed access to mobile phones / other electronic devices which may have 3G or 4G accessibility during the School day unless they are being used to enhance learning and under the direct supervision of a teacher. Sixth Form students are allowed access to mobile phones / other electronic devices within the Sixth Form centre. Such devices may have 3G / 4G accessibility and therefore the School’s filtering systems are redundant. The Sixth Form PSHCEE curriculum covers topics such as staying safe on line, sexting, the threat of radicalisation, child sexual exploitation in the hope of educating students of the potential risks associated with emerging technologies.

Managing the Internet

- The School provides pupils with access to Internet resources (where reasonable) through the School’s fixed and mobile internet connectivity
- Staff will preview any recommended sites, online services, software and apps before use
- If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents will be advised to supervise any further research
- All users must observe software copyright at all times. It is illegal to copy or distribute School software or illegal software from other sources
- All users must observe copyright of materials from electronic resources

Data storage

The School takes its compliance with GDPR seriously.

Staff and pupils are expected to save all data relating to their work to their personal home drive on the School network or appropriate part of the shared drive on the School's central server.

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the e-Safety Coordinator.

Complaints

As with all issues of safety at the School, if a member of staff, a pupil or a parent / carer has a complaint or concern relating to e-safety prompt action will be taken to deal with it. Complaints should be addressed to the e-Safety Coordinator in the first instance, who will undertake an immediate investigation and liaise with the Senior Leadership Team and any members of staff or pupils involved. Please see the Complaints Policy for further information.

Incidents of or concerns around e-safety will be recorded using a Record of Conversation Form and reported to the School's e-Safety Co-ordinator and the DSL in accordance with the School's Child Protection Policy.

Breach of this Policy

A breach or suspected breach may result in the temporary or permanent withdrawal of School ICT hardware, software or services, disciplinary action for staff, sanctions for pupils and possible criminal/civil proceedings.

Disposal of Redundant ICT Equipment Policy

- All redundant ICT equipment will be disposed of through an authorised agency. This should include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data
- All redundant ICT equipment that may have held personal data will have the storage media over written multiple times to ensure the data is irretrievably destroyed. Or if the storage media has failed it will be physically destroyed. The School will only use authorised companies who will supply a written guarantee that this will happen
- Disposal of any ICT equipment will conform to all current legislation.
- The School will maintain a comprehensive inventory of all its ICT equipment including a record of disposal
- The School's disposal record will include:
- Date item disposed of
- Authorisation for disposal, including:
  - verification of software licensing
  - any personal data likely to be held on the storage media*
- How it was disposed of e.g. waste, gift, sale
- Name of person & / or organisation who received the disposed item

* if personal data is likely to be held the storage media will be over written multiple times to ensure the data is irretrievably destroyed.

Past Staff and Pupils

All email accounts are disabled once a pupil or member of staff leaves the School.

Head Teacher: Nicola Smillie

Signature:_______________________________ Date:__________________

Chair of the Governing Body; Carol McNidder

Signature:_______________________________ Date:__________________

March 2017	**Section on Techncial Provsion added**
March 2017	**Head added as e-Safety Co-ordinator**
Sept 2018	**Deputy Head (DSL) added as e-Safety Co-ordinator**
Sept 2018	**Sections on safe use of images and AUP removed to create new policy**
Sept 2018	

Saint Martin's

Saint Martin's iPad Loan Agreement

While any equipment belonging to Saint Martin's School ("School") is in your care, the following items should be noted:

- The equipment is the property of the School and is only for use by the Department or member of staff it is issued to. Department Heads are responsible for keeping track of who within their department has possession of the iPad. Where an iPad is allocated to two Heads of Department or two or more members of staff i/c a subject they are all equally responsible for keeping track of the whereabouts of the iPad
- Pupils may use a school/department iPad in school time under supervision of a member of staff
- Length of loan is currently open and will be reviewed by the Leadership Team as the development of the use of iPads continues within School
- Users should follow all the setup instructions issued by the ICT Network Team. Following these steps will ensure the device is properly configured to work with the School's Wi-Fi
- Any iPad issued to staff remains the property of the School. IPads must be returned in a good state of repair and before departure if you are no longer employed by the School
- IPads should only be used for tasks related to the School and not for personal use
- IPads are primarily for use within School. However:
- IPads may be taken offsite to enable pupils to learn outside of the classroom, for example on School trips
- IPads may be taken offsite to carry out lesson preparation, attend training etc.
- IPads should not be taken on holiday or abroad without the permission of the Head
- IPads may be connected to home Wi-Fi connections to provide access to the internet. However, users should ensure the appropriate firewall and security features are enabled on the router before connection
- IPads may be connected to public hotspots to enable Internet access if required. However, users should be aware of the potential unsecure nature of public hotspots and ensure their activity is limited accordingly. Public hotspots should not be used to send confidential or secure information
- Users should always log out of apps and services which provide remote access into the School network after use
- If instructed to do so, staff should sign up for an Apple ID using their School email address. This will ensure apps paid for the by the School can be easily deployed to the appropriate member of staff
- Any charges related to accessing the internet from home or purchasing Apps are not chargeable to the School although HODs may choose to designate some of their departmental budget to the installation of apps
- Users should not delete any apps that are already installed on the iPad
- IPads should never be left unattended in cars or other public areas
- Users should not change the name of the iPad
- The member of staff to which an iPad has been assigned is responsible for:
- all the content on the iPad including photos and documents saved
- ensuring that the iPad is stored safely out of sight whether in School or offsite
- IPads should be protected by ensuring devices auto-lock after a period of inactivity and require a password or passcode to unlock. Any password should be notified to the Network Manager
- Should any faults occur or any other problems or issues be encountered, the School's ICT Network Team must be advised as soon as possible. Under no circumstances should staff attempt to fix any suspected hardware or software faults
- As iPads will connect to the School network and may access potentially sensitive information staff should ensure care is taken to make certain data remains confidential

- IPads may be recalled and inspected by the Network Team at any time
- If staff are found to be using an iPad in an inappropriate or irresponsible manner, which results in damage to the iPad, they may be required to replace the iPad or contribute towards a replacement
- In the event an iPad is lost or stolen, a member of the ICT Network Team should be contacted immediately to ensure all remote services can be blocked or reset.
- Upon request, the iPad should be returned to the ICT Network Team to allow maintenance and upgrades to be carried out
- Staff should be aware that the conditions outlined in the E-Safety Policy and Acceptable Use Policy also apply to iPads
- Staff should not synchronise the School iPad to any computer

Insurance

- Under the School's Combined Insurance cover there is an extension called "Temporary Removal". This provides insurance in respect of contents whilst they are temporarily removed from the School premises, provided they are in the custody or control of a member of staff
- Damage or loss arising out of theft or attempted theft from an unattended vehicle will not be covered unless all doors, windows and other points of access have been closed and locked, any other security devices correctly set to operate, and all keys removed from the vehicle
- You are responsible for maintaining the equipment in good condition and will return the equipment to the School if repairs are necessary
- You are advised to comply with the School insurer's requirements as set out above and if the IT equipment is damaged, lost or stolen, the School may deduct the cost of repair/replacement from your pay whether that be the excess only or the full replacement value of the IT equipment
- Immediately upon the termination of your employment (howsoever arising), you will return any equipment to the School in good condition. If, following an inspection by the School, it transpires that the equipment has been damaged by your negligence or misuse, you will be expected to bear the cost for all repairs that the School deems necessary, which may be deducted from your pay
- As set out above, the School has the right to deduct certain costs in respect of the loaned equipment from your pay and your signature to the Agreement constitutes your consent to the provision.

Saint Martin's Staff iPad Loan Information

Product details:	
Name:	Department:
Date Loaned:	Date Returned:

I confirm that I have read and understood the iPad Loan Agreement and will comply with it, the School's E-Safety and Acceptable Use Policies.

Signed:

Date:

Copy 1: to be retained by Network Team
Copy 2: to be retained by Member of Staff

Saint Martin's

Staff Consent Form for permission to photograph(s)/words

Use of photograph(s)/words

Your photograph(s)/words will be used solely to promote the activities of Saint Martin's and may appear in any of our promotional material in printed or electronic form including web sites, in multimedia productions, prospectuses or School magazines. Please note that websites can be seen worldwide and not just in the UK where UK law applies.

GDPR

To comply with the Regulations, we need your permission before we take any photographs or use your words. We will normally store photographs/words securely in our image library for no longer than 5 years and your consent will expire after this period.

However your photograph(s)/words may be selected for inclusion in our historical archive and be retained indefinitely.

Consent

Please provide the information requested below and give us your consent to use your photograph(s)/words in accordance with the purposes.

A full copy of the School's policy on e-safety can be found on the School website.

Please read the questions below, circle your answers and then sign and date the bottom of the form.

1 Can we use your photograph(s)/words within School, and display this within the School? **YES / NO**

2 Can we use your photograph(s)/words in printed publications eg School prospectus? **YES / NO**

3 Can we use your photograph(s)/words on our website and social media sites eg Facebook / Twitter? **YES / NO**

4 Can we use your photograph(s)/words for publication in a newspaper? **YES / NO**

5 Can we video you, for example in School productions and concerts? These DVDs may be available for sale to parents. **YES / NO**

Name: ___________________________________

Signed: ____ Date: _____________

Please then return this form to the HR Manager by date: ....

E-Safety Incident Log

This is a record of ALL eSafety incidents reported to the eSafety Coordinator. This incident log will be monitored termly by the Senior Leadership Team and the Nominated Governor. Any incidents involving Cyberbullying will also be recorded on the Bullying Register.

Date & Time	Name of pupil or staff member	Room and computer / device number	Details of incident (including names of anyone involved and evidence)	Actions, reasons and outcome	Signed