e-Safety Policy

Date for renewal/updates/review	February 2023
Named person responsible for monitoring	Business Manager
Agreed by Finance, Premises, Health & Safety Committee	February 2020

1. Contacts

- **Designated Safeguarding Lead (DSL):** Assistant Headteacher (Tel: 01494 815211 ex 205)
- **Additional Designated Safeguarding Lead (ADSL):** Inclusion Manager (Tel: 01494 815211 ex 285)
- **E-Safety Officer:** ICT Manager (Tel: 01494 815211 ex 340)
- **Nominated e-safety Governor:** Safeguarding Governor

2. Policy Statement

For clarity, the e-safety policy uses the following terms unless otherwise stated:

Users - refers to staff, governing body, school volunteers, students and any other person working in or on behalf of the school, including contractors.

Parents – any adult with a legal responsibility for the child/young person outside the school e.g. parent, guardian, carer.

School – any school business or activity conducted on or off the school site, e.g. visits, conferences, school trips etc.

Wider school community – students, all staff, governing body & parents

Safeguarding is a serious matter; at Sir William Ramsay School we use technology and the Internet extensively across all areas of the curriculum. Online safeguarding, known as e-safety, is an area that is constantly evolving and as such this policy will be reviewed on an annual basis or in response to an e-safety incident, whichever is sooner.

The primary purpose of this policy is twofold:

- To ensure the requirement to empower the whole school community with the knowledge to stay safe and risk free is met.
- To ensure risks are identified, assessed and mitigated (where possible) in order to reduce any foreseeability of harm to the student or liability to the school.

3. Policy Governance (Roles & Responsibilities)

3.1 Governing Body

The Governing Body is accountable for ensuring that our school has effective policies and procedures in place; as such they will:

- Review this policy at least annually and in response to any e-safety incident to ensure that the policy is up to date, covers all aspects of technology use within the school, e-safety incidents were appropriately dealt with and the policy was effective in managing those incidents.
- Appoint one governor to have overall responsibility for the governance of e-safety at the school who will:
    - Keep up to date with emerging risks and threats through technology use.
    - Receive regular updates regarding training, identified risks and any incidents.

3.2 Headteacher

Reporting to the Governing Body, the Headteacher has overall responsibility for e-safety within our school. The day-to-day management of this will be delegated to a member of staff, the e-Safety Officer, as indicated below.

The Headteacher will ensure that:

- E-Safety training throughout the school is planned and up to date and appropriate to the recipient, i.e. students, all staff, senior leadership team and governing body, parents.
- The designated e-Safety Officer has had appropriate CPD in order to undertake the day to day duties.
- All e-safety incidents are dealt with promptly and appropriately.
- There are appropriate processes to enable effective reporting of incidents.

3.3 e-Safety Officer

The day-to-day duty of the e-Safety Officer is devolved to the Designated Safeguarding Lead (DSL) with support from the ICT Network Manager. In the absence of the DSL, any concerns should be reported to one of the Deputy Designated Safeguarding Leads.

The e-Safety Officer will:

- Keep up to date with the latest risks to students whilst using technology; be familiar with the latest research and available resources for school and home use.
- Review this policy regularly and bring any matters to the attention of the Headteacher.
- Advise the Headteacher and Governing Body on all e-safety matters.
- Engage with parents and the school community on e-safety matters at school and/or at home.
- Liaise with the local authority, IT technical support and other agencies as required.
- Retain responsibility for the e-safety incident log; ensure staff know what to report and ensure the appropriate audit trail.
- Ensure any technical e-safety measures in school (e.g. Internet filtering software, behaviour management software) are fit for purpose through liaison with the ICT Network Manager.
- Liaise with the ICT Network Manager in relation to any reporting functions with technical e-safety measures, i.e. internet filtering reporting function; liaise with the Headteacher and responsible governor to decide on what reports may be appropriate for viewing.

- Liaise with the ICT Network Manager to ensure regular (at least termly) testing of devices and measures installed on the school's systems to ensure that they work as specified and that it isn't possible to bypass security systems. The ICT Manager will record these checks electronically.

3.4 ICT Network Manager

The ICT Network Manager is responsible for ensuring that:

- The IT technical infrastructure is secure; this will include at a minimum:
  - Anti-virus is fit-for-purpose, up to date and applied to all capable devices.
  - Windows (or other operating system) updates are regularly monitored and devices updated as appropriate.
  - Any e-safety technical solutions such as Internet filtering are operating correctly.
  - Filtering levels are applied appropriately and according to the age of the user; that categories of use are discussed and agreed with the e-safety officer and Headteacher.
  - Passwords are applied correctly to all users regardless of age. Passwords for staff will be a minimum of 8 characters.

3.5 All Staff

Staff are to ensure that:

- All details within this policy are understood. If anything is not understood it should be brought to the attention of the DSL/ADSL or Headteacher.
- Any e-safety incident is reported to the e-Safety Officer (and an e-Safety Incident report is made), or in their absence a ADSL or Headteacher.
- The reporting processes contained within this e-safety policy are fully understood.

3.6 All Students

- The boundaries of use of ICT equipment and services in this school are given in the student Acceptable Use Policy; any deviation or misuse of ICT equipment or services will be dealt with in accordance with the behaviour policy.
- e-Safety is embedded into our curriculum; students will be given the appropriate advice and guidance by staff. Similarly, all students will be fully aware how they can report areas of concern whilst at school or outside of school.

3.7 Parents and Carers

- Parents play the most important role in the development of their children; as such the school will make reasonable efforts to ensure that parents have the skills and knowledge, they need to ensure the safety of children outside the school environment. Through parents' evenings, school newsletters, the school website and leaflets the school will keep parents up to date with new and emerging e-Safety risks and will involve parents in strategies to ensure that students are empowered.
- Parents must also understand the school needs have to rules in place to ensure that their child can be properly safeguarded. As such parents will sign the student Acceptable Use Policy before any access can be granted to school ICT equipment or services.

4. Technology

Sir William Ramsay School uses a range of devices including PC's, laptops, Apple Macs, iPads. In order to safeguard the student and in order to prevent loss of personal data we employ the following assistive technology:

4.1 Internet Filtering – we use Schools Broadband/Impero software that prevents unauthorized access to illegal websites. It also prevents access to inappropriate websites; appropriate and inappropriate is determined by the age of the user and will be reviewed in line with this policy or in response to an incident, whichever is sooner. The Network Manager, e-Safety Officer and IT Support are responsible for ensuring that the filtering is appropriate and that any issues are brought to the attention of the Headteacher.

4.2 Email Filtering – we use Office 365 from Microsoft that has built in tools that prevents any infected email to be sent from the school, or to be received by the school. Infected is defined as: an email that contains a virus or script (i.e. malware) that could be damaging or destructive to data; spam email such as a phishing message.

4.3 Encryption – All school devices that hold personal data (as defined by the General Data Protection Regulation (**GDPR**) (Regulation (EU) 2016/679)) are encrypted. No data is to leave the school on an un-encrypted device; all devices that are kept on school property and which may contain personal data are encrypted. Any breach (i.e. loss/theft of device such as laptop or USB data drives) is to be brought to the attention of the Headteacher immediately. The Headteacher will liaise with the Data Protection Officer to ascertain whether a report needs to be made to the Information Commissioner's Office.

4.4 Passwords – all staff and students will be unable to access any device without a unique username and password. Staff and student passwords will change on a termly basis or if there has been a compromise, whichever is sooner.

4.5 Anti-Virus – All capable devices will have anti-virus software. This software will be updated at least weekly for new virus definitions. The ICT Network Manager will be responsible for ensuring this task is carried out and will report to the Headteacher if there are any concerns. All USB peripherals such as USB data drives (if you allow them) are to be scanned for viruses before use.

5. Safe Use

5.1 Internet – Use of the Internet in school is a privilege, not a right. Internet use will be granted: to staff upon signing this e-safety and the staff Acceptable Use Policy; students upon signing and returning their acceptance of the Acceptable Use Policy.

5.2 Email – All staff are reminded that emails are subject to Freedom of Information requests, and as such the email service is to be used for professional work-based emails only. Emails of a personal nature are not permitted. Similarly use of personal email addresses for work purposes is not permitted. Students are permitted to use the school email system, and as such will be given their own email address.

5.3 Photos and videos – All parents must provide photo/video consent at the beginning of their child's time at the school; non-return of the consent form will not be assumed as acceptance. Parents will be able to change their consent at anytime.

5.4 Social Networking – there are many social networking services available. Sir William Ramsay School is fully supportive of social networking as a tool to engage and collaborate with learners, and to engage with parents and the wider school community. The following social media services are permitted for use within Sir William Ramsay School and have been

appropriately risk assessed; should staff wish to use other social media, permission must first be sought via the e-Safety Officer who will advise the Headteacher for a decision to be made. Any new service will be risk assessed before use is permitted.

- Blogging – used by staff and students in school.
- Twitter – used by the school after approval from the Head.
- Facebook – used by the school after approval from the Head.
- Instagram – used by the school after approval from the Head.

In addition, the following is to be strictly adhered to:

- Parental consent must be obtained before any image or video of any child is uploaded.
- There is to be no identification of students using first name and surname; first name only is to be used.
- Where services are "comment enabled", comments are to be sent to "moderated".
- All posted data must conform to copyright law; images, videos and other resources that are not originated by the school are not allowed unless the owner's permission has been granted or there is a licence which allows for such use (i.e. creative commons).

5.5 Notice and take down policy – should it come to the school's attention that there is a resource which has been inadvertently uploaded, and the school does not have copyright permission to use that resource, it will be removed within one working day.

5.6 Incidents - Any e-safety incident is to be brought to the immediate attention of the e-Safety Officer, or in his absence the DSL/ADSL or Headteacher. The e-Safety Officer will assist you in taking the appropriate action to deal with the incident and to fill out an incident log.

5.7 Training and Curriculum - It is important that the wider school community is sufficiently empowered with the knowledge to stay as risk free as possible whilst using digital technology; this includes updated awareness of new and emerging issues. As such, Sir William Ramsay School will have an annual programme of training which is suitable to the audience. As well as the programme of training we will establish further training or lessons as necessary in response to any incidents. The e-Safety Officer is responsible for recommending a programme of training and awareness for the school year to the Headteacher and responsible Governor for consideration and planning. Should any member of staff feel they have had inadequate or insufficient training generally or in any particular area this must be brought to the attention of the Headteacher for further CPD.

E-Safety for students is embedded into the curriculum; whenever ICT is used in the school, staff will ensure that there are positive messages about the safe use of technology and risks as part of the student's learning.