REDMAIDS' HIGH SCHOOL
FOR GIRLS | BRISTOL

CODE OF PRACTICE

ONLINE SAFETY

To be read in conjunction with: *Anti-bullying policy, Behaviour and Sanctions, Safeguarding and child protection, ICT Staff iPad Acceptable Use Agreement, ICT Staff Acceptable Use Agreement, PSHE Scheme of work, Safer Working Practice Behaviour and Code of Conduct, Student Mobile Device and ICT Acceptable Use in Senior School, ICT Acceptable Use Policy for Year 3-6, Mobile phone guidelines for pupils in Junior School, Data Protection and privacy notices and the Employment Manual – social media policy.*

Applicable to: All members of the school community, including staff, students, parents, governors, supply staff or visitors who have access to the school ICT network, both in and out of school and who use ICT.

The policy relates to use of technology, including:

- Email
- Internet use
- The Hub – Virtual Learning Environment
- Video conferencing software e.g. Teams and Zoom
- Shared and collaborative workspaces e.g. Microsoft 365 online
- Social networking e.g. Snapchat, Instagram, etc.
- Use of PCs and mobile devices, including smartwatches
- Video hosting sites e.g. YouTube and Click View

It applies to the use of any of the above on school premises and also any use, whether on or off school premises, which affects the welfare of other students or puts the school's reputation at risk. This policy has been put together using the 360 Safe online safety self-review tool (https://360safe.org.uk/). The tool is intended to help schools review their online safety policy and practice.

Aims

- To encourage students to make good use of the educational opportunities presented by the internet and other electronic communication
- To ensure that students are ICT literate and can use facilities to ensure that their educational provision is enhanced
- To safeguard and promote the welfare of the students by preventing 'cyber bullying', grooming and other forms of abuse.
- To help students take responsibility for their own e-safety
- To ensure that students use technology safely and securely
- To ensure support for families' e-safety at home
- To provide training to staff and monitor its impact

Issues

The use of these technologies in school and at home has been shown to raise educational standards and to promote student achievement. Technology can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. However, the use of some of these technologies can put young people at risk within and outside school. It should also be remembered that there is a potential for excessive use which may impact on the social and emotional development and the learning of the young person.

The issues classified within online safety are considerable but can be categorised into four areas:

- **content**: being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.

- **contact**: being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes'.

- **conduct**: personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying; and

- **commerce** - risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group (https://apwg.org/).

Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within Redmaids' High School.

Governors

Governors are responsible for the approval of the Online Safety code of practice and for reviewing the effectiveness of the document. This will be carried out by the Governors receiving regular information about online safety incidents and monitoring reports. A member of the Governing Body has taken on the role of Online Safety Governor. The role of the Online Safety Governor will include:

- regular meetings with the Online Safety Co-ordinator
- regular monitoring of online safety incident logs and filtering/change control logs
- reporting to relevant Governor Committee meetings

Head/Headteacher

- The Head/Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the Online Safety Officer.
- The Head/Headteacher and (at least) another member of the Senior Management Team (SMT) should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
- The Head/Headteacher is responsible for ensuring that the Online Safety Officer and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Head/Headteacher will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Senior Management Team will receive regular monitoring reports from the Online Safety Officer.

Online Safety Officer

- leads the Online Safety Group
- takes day to day responsibility for online safety issues and has a leading role, with the Compliance Officer, in establishing and reviewing the school online safety policies/ documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- Highlights training needs and advises staff
- liaises with the Local Authority / MAT / relevant body
- liaises with school technical staff, as necessary
- Receives, alongside the Compliance Officer, reports of online safety incidents and oversees a log of incidents to inform future online safety developments
- meets regularly with Online Safety Governor to discuss current issues, review incident logs and filtering control logs
- reports regularly to SMT

Head of IT Infrastructure is responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets required online safety technical requirements and any Local Authority/MAT/other relevant body Online Safety Policy/ Guidance that may apply.
- the filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant

- that the use of the network/internet/The Hub/remote access/email is regularly monitored in order that any misuse or attempted misuse can be reported to the Head/Headteacher and Online Safety Officer for investigation, action or sanction
- that monitoring software and systems are implemented and updated as agreed in school policies

Teaching and Support Staff

Are responsible for ensuring that:

- they have an up-to-date awareness of online safety matters and of the current school Online Safety Policy and practices
- they have read, understood and signed the ICT Staff Acceptable Use Agreements
- they report any suspected misuse or problem to the Head/Headteacher and Online Safety Officer for investigation, action or sanction
- all digital communications with students/pupils/parents/carers should be on a professional level and only carried out using official school systems
- online safety issues are embedded in all aspects of the curriculum and other activities
- students/pupils understand and follow the ICT Acceptable Use Agreement
- students/pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned students/pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Designated Safeguarding Lead

Should be trained in Online Safety issues and be aware of the potential for serious child protection and safeguarding issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- online-bullying

Online Safety Group

The Online Safety Group provides a consultative group that has wide representation from the school community, with responsibility for issues regarding online safety and the monitoring the Online Safety code of practice including the impact of initiatives. The group will also be responsible for regular reporting to the Governing Body. The group will consist of the Online Safety Officer, The Head of

Computer Science, The DSLs, The Compliance Officer and the Head of IT Infrastructure. This group will meet termly and feed into the Education and Safeguarding Governors' Meeting.

Members of the Online Safety Group will assist the Online Safety Officer with:

- the production/review/monitoring of the school Online Safety code of practice and acceptable use documents (Compliance Officer).
- the production/review/monitoring of the school filtering policy and requests for filtering changes (Head of IT Infrastructure).
- mapping and reviewing the online safety/digital literacy curricular provision – ensuring relevance, breadth and progression (Online Safety Officer)
- monitoring network/internet/incident logs (Head of IT Infrastructure)
- consulting stakeholders – including parents/carers and the students/pupils about the online safety provision (Head of IT)
- monitoring improvement actions identified through use of the 360 degree safe self-review tool (all)

Students/Pupils:

- are responsible for using the school digital technology systems in accordance with the ICT Acceptable Use Agreement
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking/use of images and on online-bullying.
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety code of practice covers their actions out of school, if related to their membership of the school
- should be aware that the online safety code of practice also covers their actions <u>out of school</u>

Parents and Carers

Parents and Carers play a crucial role in ensuring that their children understand the need to use the internet and mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, Friday Bulletin, letters, the Hub, information about national and local online safety campaigns. Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of digital and video images taken at school events, access to parents' sections of the Hub and on-line student/pupil records and their children's personal devices in the school.

Education

Education – Students/Pupils

The education of students/pupils in online safety and digital literacy is an essential part of the school's online safety provision. Students/pupils need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Online safety is a focus in all areas of the curriculum and staff reinforce online safety messages across the curriculum. The online safety curriculum is broad, relevant and provides progression, with opportunities for creative activities and will be provided in the following ways:

- A planned online safety curriculum is provided as part of PHSE lessons and is regularly revisited
- Key online safety messages will be reinforced by all subject staff as part of lessons, assemblies and tutor time activities which will cover both the use of ICT and technology in school and outside school
- Students will be taught by subject staff in all subject areas to be critically aware of the materials/content they access online and be guided to validate the accuracy of the information
- Students will be helped to understand the need for the student ICT Code of Practice and encouraged to adopt safe and responsible use of the internet, of ICT and PCs and mobile devices both within and outside school.
- In lessons where internet use is pre-planned, it is good practice for teaching staff to guide students to sites checked as suitable for their use; staff should be vigilant about monitoring the content that students access online and the websites they visit.
- Students are taught across all subject areas to acknowledge the source of information used and to respect copyright when using materials accessed on the internet.
- Students are encouraged to write Social Media charters in their tutor groups to encourage the responsible use of these platforms. These are overseen by the Heads of Year and the e-Safety Coordinator and will coincide with Safer Internet Day (February).
- Students / pupils should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Education – Parents/Carers

Parents and carers play an essential role in the education of their children and in the monitoring and regulation of the children's online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through online safety events, for example, pastoral evenings for parents, Friday Bulletin, The Hub, email and letters.

Education – The Wider Community

The school will provide opportunities for local members of the community to gain from the school's online safety knowledge and experience through the Bristol Education Partnership and elsewhere, as possible.

Education & Training – Staff

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.
- All new staff will be asked to read and fully understand the school Online Safety Code of Practice and sign the ICT Acceptable Use Agreements
- This Online Safety Policy and its updates will be highlighted to staff and the Online Safety Officer will provide advice to individuals as required.

Training – Governors

The nominated online safety governor should take part in online safety training and awareness sessions, such as ISBA courses or participation in school training sessions for staff or parents.

Technical – infrastructure, equipment, filtering and monitoring

The school will be responsible for ensuring that the school network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:

- There will be regular reviews and audits of the safety and security of school technical systems

- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school technical systems and devices.
- All users (at KS2 and above) will be provided with a username and secure password by the IT Department who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password and will be required to change their password every 90 days).

- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes
- Internet filtering and monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet.
- School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.
- An appropriate system is in place for users to report any actual or potential technical incident or security breach to the relevant person, as agreed).
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- Good practice is in place for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the school systems.
- An agreed policy is in place Staff iPad Acceptable Use Policy and ICT Acceptable Use Policy regarding the extent of personal use that users (staff / students / pupils / community users) and their family members are allowed on school devices that may be used out of school.
- There is a system policy set on the servers forbids staff from downloading executable files and installing programmes on school devices.
- An agreed policy is in place regarding the use of removable media (e.g. memory sticks / CDs / DVDs) by users on school devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Sanctions

Senior School

Girls who do not observe the ICT Code of Practice may expect a temporary or permanent ban on use of the internet, email and/or ICT facilities. Additional disciplinary action of a more serious nature may also be expected. Most initial offences will be dealt with by the Assistant Head (Pastoral) and parents will be notified. Should serious cases of e-safety incidents take place; the police will be informed as appropriate. The school's DSL will be informed and procedures will be followed when there are concerns over safeguarding and child protection issues.

Junior School

Pupils who do not observe the code of conduct have their iPad removed and it is left on the Headteacher's desk to be collected with the parent at the end of the day. Parents are informed. Repeat misdemeanour would lead to a longer time of removal and sanctions following our behaviour policy. Should serious cases of e-safety incidents take place; the police will be informed as appropriate. The school's DSL will be informed and procedures will be followed when there are concerns over safeguarding and child protection issues.

Online Safety Group (OSG)

Governor – Abdul Farooq
Online Safety Officer – Alice Hinks
The Head of Computer Science – Senior School – Connor Kelly
DSLs – Jackie Turner, Lisa Brown
DDSLs – Kate Doarks, Jo Marsden, Julie Owens-Powell, Jon Cooper, Alison Weeks
Head of IT Infrastructure – Sarah Bramley-Dymond
Compliance Officer – Lucy Malt

Reviewed by Online Safety Group June 2021
Review date June 2022

Appendix 1

Year Group	Learning Objectives
Year 2, 3 & 4 (biannual cycle)	• ICT Code of Conduct (every year) • e-safety – the SMART rules • e-safety • NSPCC
Year 5 & 6 (biannual cycle)	• ICT Code of Conduct (every year) • 'Play like and share' CEOP internet online safety training • How to communicate on-line • Social media Anti-bullying • NSPCC
Year 7	• Explore cyber bullying and its effects on individuals (PSHE) • To learn about the possible isolation caused by social media/WhatsApp groups when settling in to new schools • To learn how to conduct healthy relationships online (PSHE) • To learn how to respond to and manage negative online relationships (PSHE) • Internet safety/ cyber bullying – Computer Science • Phishing and dangers – Computer Science • To understand what fake news is, why it is created. • Understand how fake news can affect people's emotions and behaviours (Computer Science) • Understand how to search the web safely and securely – Computer Science • Internet safety week lesson
Year 8	• To understand the impact of social media on body ideals and the negative impact on body positivity (PSHE) • Internet safety week lesson
Year 9	• Cyber Crime – Understand the various threats related to being online – Computer Science. • To understand the various forms of attacks online and ways to prevent these attacks – Computer Science. • Social media and cyber bullying – Computer Science • Internet safety week lesson
Year 10 & 11	• To learn how to manage their digital footprint (PSHE) • To learn how to handle unwanted attention, including stalking and trolling online (PSHE) • Learn about the safe and responsible use of mobile phones during a gun or knife attack (PSHE)

	• Learn the criminal implications of sexting and sending nude imagery (PSHE) • Cultural, legal, moral, ethical and environmental issues related to computing and being online. - Computer Science • Threats to a network and online safety - Computer Science • Legislation related to computer science – Data protection act, computer misuse act, copyright design and patent act, freedom of information act.
Year 12	• Online reputation and digital footprint (Futures) • Build on cybercrime – various forms of attacks/threats and ways to prevent these.
Year 13	• Build on the Cultural, legal, ethical, moral, environmental issues related to being online and computing. • Build on Legislation related to computer science – Data protection act, computer misuse act, copyright design and patent act, freedom of information act.

Appendix 2 - Resources

UK Safer Internet Centre
Safer Internet Centre – https://www.saferinternet.org.uk/
South West Grid for Learning - https://swgfl.org.uk/products-services/online-safety/
Childnet – http://www.childnet-int.org/
Professionals Online Safety Helpline - http://www.saferinternet.org.uk/about/helpline
Internet Watch Foundation - https://www.iwf.org.uk/

CEOP
CEOP - http://ceop.police.uk/
ThinkUKnow - https://www.thinkuknow.co.uk/

Others
LGfL – Online Safety Resources
Kent – Online Safety Resources page
INSAFE / Better Internet for Kids - https://www.betterinternetforkids.eu/
UK Council for Child Internet Safety (UKCCIS) - www.education.gov.uk/ukccis
Netsmartz - http://www.netsmartz.org/
National Cyber Security Centre - https://www.ncsc.gov.uk/
South West Cyber Security Cluster - https://southwestcsc.org/

Tools for Schools
Online Safety BOOST – https://boost.swgfl.org.uk/
360 Degree Safe – Online Safety self-review tool – https://360safe.org.uk/
360Data – online data protection self-review tool: www.360data.org.uk