Fair Ways Schools
E-Safety Policy

Document Ref:	Version No:	Summary of Changes:	Author	Release Date:	Approved By:
SC16	1	Launch	Gareth Webb	December 2015	
For details of versions 2-11 refer to control schedule at end of policy.					
GSG16	12	Review 2024/2025	Emma Moore	October 2024	PSC
GSC16	13	Removed all references to 'E-Safety Coordinators'	Laura Rowe	March 2025	PSC
SC 16	14	Reviewed and updated in line with current legislation and statutory guidance, including KCSIE 2026, DfE filtering and monitoring standards, UK GDPR/Data Protection Act 2018, cyber security standards and the Online Safety Act 2023	Victoria Adams	October 2026	QSGC

Review Date: October 2027 (Annually)
Contributor: IT Department

Contents

1 Introduction 5

2 Monitoring 6

3 Breaches 7

4 Incident Reporting 7

5 Computer Viruses 7

6 Email 8

7 Managing emails 8

8 Sending Emails 9

9 Receiving Emails 10

10 Emailing Personal, Sensitive, Confidential or Classified Information 10

11 Equal Opportunities 10

12 E-Safety - Roles and Responsibilities 11

13 E-Safety in the Curriculum 11

14 E-Safety Skills Development for Members of Staff 12

15 Managing the School E-Safety Messages 13

16 Incident Reporting, E-Safety Incident Log & Infringements 13

17 E-Safety Incident Log 13

18 Misuse and Infringements 14

19 Internet Access 14

20 Infrastructure 15

21 Managing Other Web 2 Technologies 16

22 Parental Involvement 17

23 Passwords and Password Security 18
24 Safe Use of Images 19
25 Webcams and CCTV 20
26 School ICT Equipment including Portable & Mobile ICT Equipment & Removable Media 21
27 Social Media, including Facebook and Twitter 23
28 Telephone Services 24
29 Staff Training 24
30 Current Legislation 25
31 Remote Learning 29
32 Associated Documentation & Legislation 29
Appendix A – Parent letter 32
Appendix B - Acceptable Use Agreement: Pupils – Secondary 33
Appendix C - Acceptable Use Agreement / Code of Conduct: Staff and Visitors 34
Appendix D - Flowcharts for Managing an e-Safety Incident 36

Fair Ways Vision, Mission and Values

Our vision
To build a community that changes lives, makes a difference to society and leaves a legacy greater than us and our contributions.

Our mission
To grow a compassionate, resilient, and trauma-informed community, that embraces learning, so that we improve the lives and outcomes of individuals.

Our values
Our values form the heart of the work we do, defined by Fair Ways people, for Fair Ways people. These are the values by which we operate, by which we are governed, and to which we are held accountable.

We therefore expect every individual within the organisation to *play their part*:

PROFESSIONAL	**A**CCEPTING	**R**EFLECTIVE	**T**RANSPARENT
· We do what we say we will. · We approach challenges with optimism and enthusiasm. · We don't judge, we notice. · We put the needs of the service before our own personal gains.	· We don't give up on people. · We value all individuals and are willing to challenge them. · We embrace each other's differences as much as our similarities. · We accept responsibility for our actions.	· We give feedback, we invite feedback, we listen to feedback. · We look inward before we look outward. · We learn as much from our mistakes as from our successes. · We listen to each other, learn from each other and grow together.	· We are always willing to explain why. · We have the courage to be open and honest. · We earn trust through our transparency. · We live by our values even when no-one is watching.

1 Introduction

1.1 Information and Communications Technology (ICT) in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, students and adults. Consequently, schools need to build, in the use of these technologies in order to arm our students with the skills to access life-long learning and employment.

1.2 Information and Communications Technology covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently, the internet technologies children and students are using both inside and outside of the classroom include:

- websites
- email, Instant Messaging and chat rooms
- social media, including X (Facebook), TikTok and Instagram
- mobile / smart phones with text, video and / or web functionality
- other mobile devices with web functionality
- gaming, especially online
- learning platforms and Virtual Learning Environments
- blogs and Wikis
- podcasting
- video broadcasting
- music downloading

1.3 Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies and that some have minimum age requirements, usually 13 years.

1.4 Within Education we understand the responsibility to educate our students on e-Safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

1.5 Everybody in the schools have a shared responsibility to secure any sensitive information used in their day-to-day professional duties and even staff not directly involved in data handling should be made aware of the risks and threats and how to minimise them.

1.6 Both this policy and the Acceptable Use Agreement (for all members of staff, Directors, visitors and students) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, mobile devices, webcams, whiteboards, voting systems, digital video equipment, etc.); and technologies owned by students and staff, but brought onto school premises (such as laptops, mobile phones, and other mobile devices).
(Refer Appendix B – Acceptable Use Agreement Pupils & Appendix C Acceptable Use Agreement- Code of Conduct: Staff and Visitors)

2 Monitoring

2.1 The IT Department may inspect any ICT equipment owned or leased by the school at any time without prior notice. If you are in doubt as to whether the individual requesting such access is authorised to do so, please ask for their identification badge and contact their department. Any ICT authorised staff member will be happy to comply with this request.

2.2 The school will maintain appropriate filtering and monitoring systems in line with statutory safeguarding guidance and the Department for Education digital and technology standards. Filtering is preventative and helps block illegal, inappropriate and potentially harmful content, including AI-generated content where relevant. Monitoring is reactive and supports staff to identify and respond to potential safeguarding concerns.

2.3 Filtering and monitoring arrangements will be reviewed and documented at least once every academic year. The review will be led by the senior leadership team member responsible for filtering and monitoring, with support from the Designated Safeguarding Lead and IT support, and will consider the needs of students and staff, mobile and off-site access, apps, encrypted traffic, emerging technology and generative AI.

3 Breaches

3.1 A breach or suspected breach of policy by a school employee, contractor or student may result in temporary or permanent withdrawal of school ICT hardware, software or services from the offending individual.

3.2 Any policy breach is grounds for disciplinary action in accordance with the school Disciplinary Procedure.

3.3 Policy breaches may also lead to criminal or civil proceedings.

4 Incident Reporting

4.1 Any security breach, attempted breach, loss of equipment, unauthorised use or suspected misuse of ICT must be reported immediately to the Head of School, Deputy Head, Designated Safeguarding Lead and/or the nominated online safety rep, these must then be reported to the Executive Head. Where the concern involves safeguarding, online harm, illegal content, child-on-child abuse, AI-generated harmful content, sharing of images, data loss or cyber security, the school's safeguarding, data protection and incident reporting procedures must be followed without delay. Refer to Appendix D – Flowchart for Managing an E-Safety Incident.

5 Computer Viruses

5.1 All files downloaded from the Internet, received via email or on removable media such as a memory stick, must be checked for any viruses using school provided anti-virus software before being used.

5.2 Never interfere with any anti-virus software installed on school ICT equipment that you use.

5.3 If your machine is not routinely connected to the school network, you must make provision for regular virus updates through your IT team.

5.4 If you suspect there may be a virus on any school ICT equipment, stop using the equipment and contact the IT Department at it@fairways.co. The IT Department

provider will advise you what actions to take and be responsible for advising others that need to know.

6 Email

6.1 The use of email within most schools is an essential means of communication for both staff and students. In the context of school, e-mail should not be considered private. Educationally, email can offer significant benefits including; direct written contact between schools on different projects, be they staff based or pupil based, within school or international. We recognise that students need to understand how to style an email in relation to their age and good network etiquette; 'netiquette'.

7 Managing emails

7.1 The school gives all staff their own email account to use for all school business as a work-based tool. This is to protect staff, minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed.

7.2 It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary, email histories can be traced. The school email account should be the account that is used for all school business.

7.3 All emails should be written and checked carefully before sending, in the same way as a letter written on school headed paper.

7.4 Members of staff sending emails to external organisations, parents or students are advised to CC. the Head of School or their line manager.

7.5 Students may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes.

7.6 Emails created or received as part of your school job will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000. You must therefore actively manage your email account as follows:

- Delete all emails of short-term value.
- Organise email into folders and carry out frequent housekeeping on all folders and archives.
- All pupil email users are expected to adhere to the generally accepted rules of netiquette particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in email communication, or arrange to meet anyone without specific permission, virus checking attachments.
- Members of staff must inform the Deputy Head or Head of School if they receive an offensive email.
- Students are introduced to email as part of the ICT Scheme of Work.

7.7 However, you access your school email (whether directly, through webmail when away from the office or on non-school hardware) all the school email policies apply.

8 Sending Emails

8.1 If sending emails containing personal, confidential, classified or financially sensitive data to external third parties or agencies, refer to the Section 10 Emailing Personal, Sensitive, Confidential or Classified Information.

8.2 Use your own school email account so that you are clearly identified as the originator of a message.

8.3 Keep the number and relevance of email recipients, particularly those being copied, to the minimum necessary and appropriate.

8.4 Do not send or forward attachments unnecessarily. Whenever possible, send the location path to the shared drive rather than sending attachments.

8.5 School email is not to be used for personal advertising.

9 Receiving Emails

9.1 Check your email regularly.

9.2 Activate your 'out-of-office' notification when away for extended periods.

9.3 Never open attachments from an untrusted source; consult your network manager first.

9.4 Do not use the email systems to store attachments. Detach and save business related work to the appropriate shared drive / folder.

10 Emailing Personal, Sensitive, Confidential or Classified Information

10.1 Where your conclusion is that email must be used to transmit such data:

- Obtain express consent from your manager to provide the information by email.
- Exercise caution when sending the e-mail and always follow these checks before releasing the email:
  - Verify the details, including accurate email address, of any intended recipient of the information.
  - Verify (by phoning) the details of a requestor before responding to email requests for information.
  - Do not copy or forward the email to any more recipients than is absolutely necessary.
  - Do not send the information to anybody / person whose details you have been unable to separately verify (usually by phone).
  - Do not identify such information in the subject line of any email.
  - Request confirmation of safe receipt.

11 Equal Opportunities

11.1 Students with Additional Needs - The school endeavours to create a consistent message with parents for all students and this in turn should aid establishment and future development of the schools' e-Safety rules.

11.2 However, members of staff are aware that some students may require additional support or teaching including adapted resources, reminders, prompts and further explanation to reinforce their existing knowledge and understanding of e-Safety issues.

11.3 Where a student has poor social understanding, careful consideration is given to group interactions when raising awareness of e-Safety. Internet activities are planned and well managed for these students.

12 E-Safety - Roles and Responsibilities

12.1 Online safety is an important aspect of strategic safeguarding leadership within the school. The Headteacher, senior leaders, proprietors/directors and governors have responsibility for ensuring that policy, practice, training, filtering, monitoring and review arrangements are embedded and effective. Each school will identify online safety leads and a senior leadership team member responsible for filtering and monitoring. The Designated Safeguarding Lead will have appropriate understanding of online safety, filtering and monitoring systems and will work with IT support to ensure risks are identified, reviewed and acted upon.

12.2 Senior leaders and company directors will receive updates on online safety, safeguarding risks, filtering and monitoring, data protection and cyber security at least annually and whenever significant risks, incidents or changes in statutory guidance arise.

12.3 This policy, supported by the school's acceptable use agreements for staff, Directors, visitors and students, is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: child protection, health and safety, home–school agreements, and behaviour / pupil discipline (including the anti-bullying) policy and PSHE.

13 E-Safety in the Curriculum

13.1 ICT and online resources are increasingly used across the curriculum. We believe it is essential for e-Safety guidance to be given to the students on a regular and meaningful

basis. E-Safety is embedded within our curriculum, and we continually look for new opportunities to promote e-Safety.

13.2 The school has a framework for teaching internet skills in ICT lessons. Each young person has annual reviews on the skills required.

13.3 The school provides opportunities within a range of curriculum areas to teach about e-Safety.

13.4 Educating students about the online risks that they may encounter outside school is done informally when opportunities arise and as part of the E-Safety curriculum, delivered through ICT and RSHE.

13.5 Students are aware of the relevant legislation when using the internet including data protection and intellectual property which may limit what they want to do but also serves to protect them.

13.6 Students are taught about copyright, respecting other people's information, safe use of images and other important areas through discussion, modelling and appropriate activities

13.7 Students are aware of the impact of Cyberbullying including sexual and emotional abuse and know how to seek help if any form of online bullying affects them. Students are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent /carer, teacher / trusted staff member, or an organisation such as Cyber mentors, ChildLine or CEOP report abuse button.

13.8 Students are taught all aspects of safeguarding when online, including online safety, cyberbullying, harmful content, misinformation, online misogyny and harassment, image sharing, age-appropriate use, privacy, digital consent, reporting concerns and the safe and responsible use of generative AI and emerging technologies.

14 E-Safety Skills Development for Members of Staff

14.1 New members of staff receive information on the school's Acceptable Usage Policy as part of their induction.

14.2 All members of staff have been made aware of their individual responsibilities relating to the safeguarding of children within the context of E-Safety and know what to do in the event of misuse of technology by any member of the school community (see enclosed flowcharts.)

14.3 All members of staff are encouraged to incorporate E-Safety activities and awareness within their curriculum areas.

15 Managing the School E-Safety Messages

15.1 We endeavour to embed e-safety messages across the curriculum whenever the internet and / or related technologies are used.

15.2 The E-Safety policy will be introduced to the students at the start of each school year.

15.3 The key E-Safety advice will be promoted widely through school displays, newsletters and class activities.

16 Incident Reporting, E-Safety Incident Log & Infringements

16.1 Incident Reporting - Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the school's Head of School and / or E-Safety Co-ordinators. Additionally, all security breaches, lost / stolen equipment or data (including remote access SecureID tokens and PINs), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to the e-safety Co-ordinators and / or Headteacher.

16.2 If any person's report concerns which relate to safeguarding whilst online this is to be immediately reported to the school Designated Safeguarding Lead.

17 E-Safety Incident Log

17.1 Keeping an incident log can be a good way of monitoring what is happening and identify trends or specific concerns. All incidents in relation to E-safety are recorded on our Clearcare system.

18 Misuse and Infringements

18.1 Complaints and / or issues relating to E-Safety should be made to the Head of School. Incidents should be logged and the Flowcharts for Managing an E-Safety Incident should be followed.

18.2 Inappropriate Material

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the e-Safety Co-ordinators.
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the E-Safety lead, depending on the seriousness of the offence; investigation by the Headteacher/ LA. All information should be shared with the school Designated Safeguarding Lead.
- Immediate suspension, possibly leading to dismissal and involvement of police for very serious offences (see flowchart).

19 Internet Access

19.1 The internet is an open worldwide communication medium, available to everyone at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people. Whenever any inappropriate use is detected, it will be followed up.

19.2 Managing the Internet:

- The school provides students with supervised access to Internet resources (where reasonable) through the school's fixed and mobile internet connectivity.
- Staff will preview any recommended sites 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.

19.3 Internet Use:

- You must not post personal, sensitive, confidential or classified information or disseminate such information in any way that may compromise the intended restricted audience.
- Do not reveal names of colleagues, students, others or any other confidential information acquired through your job on any social networking site or other online application.
- On-line gambling or gaming is not allowed.
- It is at the Headteacher's discretion as to what internet activities are permissible for staff and students and how this is disseminated.

20 Infrastructure

20.1 School internet access is controlled through appropriate technical filtering, monitoring, firewall, anti-malware and cyber security arrangements. Systems must be capable of responding to illegal, inappropriate and potentially harmful content, including content accessed through apps and services and, where appropriate, AI-generated or dynamic content.

20.2 Members of staff and students are aware that school-based email and internet activity can be monitored and explored further if required.

20.3 If members of staff or students discover an unsuitable site, the screen must be switched off / closed and the incident reported immediately to the teacher or senior leadership as appropriate.

20.4 It is the responsibility of the school, by delegation to the network manager, to ensure that anti-virus protection is installed and kept up to date on all school machines.

20.5 Students and members of staff are not permitted to download programs or files on school based technologies without seeking prior permission from the Headteacher.

20.6 If there are any issues related to viruses or anti-virus software, the network manager should be informed.

20.7 Responsibility for filtering and monitoring is shared across the school. The senior leadership team member responsible for filtering and monitoring, the Designated Safeguarding Lead, IT support and all staff must understand their roles in recognising, reporting and responding to online safety concerns.

21 Managing Other Web 2 Technologies

21.1 Online technologies, including social networking sites, if used responsibly both outside and within an educational context can provide easy to use, creative, collaborative and free facilities. However, it is important to recognise that there are issues regarding the appropriateness of some content, contact, culture and commercialism. To this end, we encourage our students to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.

21.2 At present, the school endeavours to deny access to social networking and inappropriate online games websites to students within school. Any games accessed in school need to be age appropriate. This includes protecting against 3G and 4G use.

21.3 All students are advised to be cautious about the information given by others on such websites, for example users not being who they say they are.

21.4 Students are taught to avoid placing images of themselves (or details within images that could give background details) on such websites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online.

21.5 Students are always reminded to avoid giving out personal details on websites which may identify them or where they are (full name, address, mobile / home phone numbers, school details, IM / email address, specific hobbies / interests.)

21.6 Our students are advised to set and maintain their online profiles to maximum privacy and deny access to unknown individuals.

21.7 Students are encouraged to be wary about publishing specific and detailed private thoughts and information online.

21.8 Our students are asked to report any incidents of cyberbullying to the school.

22 Parental Involvement

22.1 We believe that 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. (Please see Appendix A). We regularly consult and discuss E-Safety with parents / carers and seek to promote a wide understanding of the benefits of new technologies together with the associated risks.

22.2 Parents / carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to the school.

22.3 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.)

22.4 Parents / carers are expected to sign a Home School agreement containing the following statement or similar:

We will support the school approach to on-line safety and not deliberately upload or add any text, image, sound or video that could upset or offend any member of the school community.

22.5 The school disseminates information to parents relating to E-Safety where appropriate in the form of:

- posters

- school website
- newsletter items

22.6 In order for all students to remain safe online it is essential there is a whole school approach from the whole school community including parents and carers.

23 Passwords and Password Security

23.1 Passwords

- **Always use your own** personal passwords.
- Make sure you enter your personal passwords each time you logon. Do not include passwords in any automated logon procedures.
- Staff should change temporary passwords at first logon.
- Change passwords whenever there is any indication of possible system or password compromise.
- Do not record passwords or encryption keys on paper or in an unprotected file.
- **Only disclose your personal password to the IT Department staff when necessary, and never to anyone else.** Ensure that all personal passwords that have been disclosed are changed once the requirement is finished.
- Never tell a child or colleague your password.
- If you are aware of a breach of security with your password or account inform the Headteacher immediately.
- If you think your password may have been compromised or someone else has become aware of your password report this to the IT Department.
-

23.2 Password Security

- Password security is essential for members of staff, particularly as they are able to access and use pupil data. Members of staff are expected to have secure passwords which are not shared with anyone. The students are expected to keep their passwords private and not to share with others, particularly their friends. Members of staff and students are regularly reminded of the need for password security.
- All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's E-Safety Policy and Data Security.

- Users are provided with an individual network, email, learning platform and **M**anagement **I**nformation **S**ystem (where appropriate) log-in username. They are also expected to use a personal password and keep it private.
- Students are not allowed to deliberately access on-line materials or files on the school network, of their peers, teachers or others.
- Members of staff are aware of their individual responsibilities to protect the security and confidentiality of the school networks, MIS systems and /or learning platform, including ensuring that passwords are not shared and are changed periodically. Individual members of staff users must also make sure that workstations are not left unattended and are locked.

23.3 Zombie Accounts refers to accounts belonging to users who have left the school and therefore no longer have authorised access to the school's systems. Such Zombie accounts when left active can cause a security threat by allowing unauthorised access.

- Ensure that all user accounts are disabled once the member of the school has left.
- Prompt action on disabling accounts will prevent unauthorized access.

24 Safe Use of Images

24.1 Taking of Images and Film:

- Digital images are easy to capture, reproduce and publish and, therefore, misuse. We must remember that it is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness.
- With the written consent of parents (on behalf of students) and staff, the school permits the appropriate taking of images by a member of staff and students with school equipment.
- Members of staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of students, this includes when on field trips.
- Students are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of students, members of staff and others without advance permission from the Headteacher.

- Students and members of staff must have permission from the headteacher before any image can be uploaded for publication.

24.2 Publishing student's images and work - On a child's entry to the school, all parents / carers will be asked to give permission to use their child's work / photos in the following ways:

- On the school web site.
- In the school prospectus and other printed publications that the school may produce for promotional purposes.
- In display material that may be used in the school's communal areas.
- In display material that may be used in external areas, i.e. exhibition promoting the school.

24.3 This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue, e.g. divorce of parents, custody issues, etc.

24.4 Parents or carers may withdraw permission, in writing, at any time. Consent has to be given by both parents in order for it to be deemed valid.

24.5 Students' names will not be published alongside their image and vice versa. Email and postal addresses of students will not be published. Students' full names will not be published.

24.6 Storage of Images:

- Images / films of children are stored on the school's network
- Students and members of staff are not permitted to use personal portable media for storage of images (e.g., USB sticks) without the express permission of the Head of School.
- Rights of access to this material are restricted to the teaching staff and students within the confines of the school network or other online school resource.

25 Webcams and CCTV

25.1 We do not use publicly accessible webcams in school.

25.2 CCTV is used to monitor the car park areas at the front and the back of the school. The company CCTV policy is adhered to and has been read by all staff.

26 School ICT Equipment including Portable & Mobile ICT Equipment & Removable Media

26.1 School ICT Equipment

- As a user of the school's ICT equipment, you are responsible for your activity.
- It is recommended that schools log ICT equipment issued to members of staff and record serial numbers as part of the school's inventory.
- Ensure that all ICT equipment that you use is kept physically secure.
- Do not attempt unauthorised access or make unauthorised modifications to computer equipment, programs, files or data. This is an offence under the Computer Misuse Act 1990.
- It is imperative that you save your data on a frequent basis to the school network.
- You are responsible for the backup and restoration of any of your data that is not held on the school's network.
- It is recommended that a time locking screensaver is applied to all machines. Any device accessing personal data must have a locking screensaver as must any user profiles.
- On termination of employment, resignation or transfer, return all ICT equipment to your manager. You must also provide details of all your system logons so that they can be disabled.
- It is your responsibility to ensure that any information accessed from your own PC or removable media equipment is kept secure, and that no personal, sensitive, confidential or classified information is disclosed to any unauthorised person.
- All redundant ICT equipment is disposed of in accordance with Waste Electrical and Electronic Equipment (WEEE) directive and Data Protection Act 2018 (DPA).
- All ICT equipment allocated to members of staff must be authorised by the appropriate Line Manager. Authorising Managers are responsible for:

    1 Maintaining control of the allocation and transfer within their Unit.
    2 Recovering and returning equipment when no longer needed.

26.2 Portable & Mobile ICT Equipment

- This section covers such items as laptops, mobile devices and removable data storage devices. Please refer to the relevant sections of this document when considering storing or transferring personal or sensitive data.
- All activities carried out on school systems and hardware will be monitored in accordance with the general policy.
- Members of staff must ensure that all school data is stored on the school network and not kept solely on the laptop. Any equipment where personal data is likely to be stored must be encrypted.
- Equipment must be kept physically secure in accordance with this policy to be covered for insurance purposes. When travelling by car, best practice is to place the laptop in the boot of your car before starting your journey.
- Ensure portable and mobile ICT equipment is made available as necessary for anti-virus updates and software installations, patches or upgrades.
- The installation of any applications or software packages must be authorised by the IT Department, fully licensed and only carried out by the IT Department.
- In areas where there are likely to be members of the general public, portable or mobile ICT equipment must not be left unattended and, wherever possible, must be kept out of sight.
- Portable equipment must be transported in its protective case if supplied.

26.3 Mobile Technologies

26.3.1 Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and students. Mobile technologies such as, Smartphones, Blackberries, iPads, games players are generally very familiar to children outside of school. They often provide a collaborative, well-known device with possible internet access and thus open up risk and misuse associated with communication and internet use. Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed. Our school chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

26.4 Personal Mobile Devices (including phones)

- The school allows members of staff to bring in personal mobile phones and devices for their own use.
- Students are allowed to bring Mobile phones for the journey to and from school, but on arrival these must be handed to the SLT team and secured in a pouch. Phones are returned to students at the end of the school day.
- The school is not responsible for the loss, damage or theft of any personal mobile device.
- The sending of inappropriate text messages between any members of the school community is not allowed.
- Permission must be sought before any image or sound recordings are made on these devices of any member of the school community.
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

26.5 **School Provided Mobile Devices (including phones)**

- The sending of inappropriate text messages between any members of the school community is not allowed.
- Permission must be sought before any image or sound recordings are made on the devices of any member of the school community.
- Where the school provides mobile technologies such as phones, laptops and iPads for offsite visits and trips, only these devices should be used.

26.6 **Removable Media**

26.6.1 Members of staff do not have the facility to use removable media on Fair Ways IT equipment. If needed a request needs to be sent to the IT department.

27 Social Media, including Facebook and Twitter

27.1 Facebook, Twitter and other forms of social media are increasingly becoming an important part of our daily lives.

27.2 Students are not permitted to access their social media accounts whilst at school.

27.3 Members of staff, students, parents and carers are regularly provided with information on how to use social media responsibly and what to do if they are aware of inappropriate use by others.

27.4 Members of staff, students, parents and carers are aware that the information, comments, images and video they post online can be viewed by others, copied and stay online forever.

27.5 Members of staff, students, parents and carers are aware that their online behaviour should at all times be compatible with UK law.

28 Telephone Services

28.1 Report the loss or theft of any school mobile phone equipment immediately.

28.2 You must read and understand the user instructions and safety points relating to the use of your school mobile phone prior to using it.

28.3 School SIM cards must only be used in school provided mobile phones.

28.4 All school mobile phones are barred from calling premium rate numbers and any numbers outside of the UK as the default.

28.5 You must not send text messages to premium rate services.

28.6 Never use a hand-held mobile phone whilst driving a vehicle. Only genuine 999 or 112 emergency calls may be made if it would be unsafe to stop before doing so.

29 Staff Training

29.1 E-Safety support will be delivered in house. The school has access to an "e-Safety and Social Media" training course on social media protection delivered on-line or by a training provider. The school also has in-house CEOP ambassadors who are responsible for cascading the Thinkuknow programme to all school staff.

30 Current Legislation

30.1 The school will comply with current statutory guidance and legislation relevant to online safety, safeguarding, filtering and monitoring, data protection and cyber security. This includes Keeping Children Safe in Education 2026, the Department for Education's digital and technology standards for filtering and monitoring and cyber security, UK GDPR and the Data Protection Act 2018, and the Online Safety Act 2023. These requirements reinforce the need for a whole-school approach to online safety, age-appropriate education, effective reporting routes, appropriate technical controls, documented reviews and clear leadership accountability.

30.2 Key current guidance includes Department for Education statutory safeguarding guidance, digital and technology standards for filtering and monitoring and cyber security, Department for Education data protection guidance for schools, UK Safer Internet Centre appropriate filtering and monitoring guidance, and Ofcom/Government guidance on the Online Safety Act.

30.3 **Acts Relating to Monitoring of members of staff email**

- **UK General Data Protection Regulation and Data Protection A**These laws require the school to process personal data lawfully, fairly, transparently and securely; maintain appropriate records and policies; protect special category and safeguarding information; respond appropriately to data subject rights and data breaches; and demonstrate accountability through regular review, training and documentation.

  http://www.hmso.gov.uk/acts/acts1998/19980029.htm

- **The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000**
  http://www.hmso.gov.uk/si/si2000/20002699.htm

- **Regulation of Investigatory Powers Act 2000**
  Regulating the interception of communications and making it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998. The Telecommunications (Lawful Business Practice) (Interception of

Communications) Regulations 2000 however, permit a degree of monitoring and record keeping, for example, to ensure communications are relevant to school activity or to investigate or detect unauthorised use of the network. Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored. Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation.
http://www.hmso.gov.uk/acts/acts2000/20000023.htm

- **Human Rights Act 1998**
  http://www.hmso.gov.uk/acts/acts1998/19980042.htm

30.4 **Other Acts Relating to E-Safety**

- **Racial and Religious Hatred Act 2006**
  It a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

- **Sexual Offences Act 2003**
  The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet). It is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. Schools should already have a copy of "*Children & Families: Safer from Sexual Crime*" document as part of their child protection packs. For more information www.teachernet.gov.uk

- **Communications Act 2003 (Section 127)**
  Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false

message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent there is no need to prove any intent or purpose.

- **The Computer Misuse Act 1990 (Sections 1 – 3)**
  Regardless of an individual's motivation, the Act makes it a criminal offence to gain:

  - Access to computer files or software without permission (for example using another person's password to access files).
  - Unauthorised access, as above, in order to commit a further criminal act (such as fraud).
  - Impair the operation of a computer or program UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

- **Malicious Communications Act 1988 (Section 1)**
  This legislation makes it a criminal offence to send an electronic message (email) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.

- **Copyright, Design and Patents Act 1988**
  Copyright is the right to prevent others from copying or using work without permission. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer. Copyright infringement is to copy all or a substantial part of anyone's work without obtaining them author's permission. Usually, a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else's material. It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.

- **Public Order Act 1986 (Sections 17 – 29)**

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006, it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

- **Protection of Children Act 1978 (Section 1)**
  It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child, for these purposes, is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

- **Obscene Publications Act 1959 and 1964**
  Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

- **Protection from Harassment Act 1997**
  A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

30.5 **Current Safeguarding, Online Safety, Data Protection and Cyber Security Requirements**

- Keeping Children Safe in Education 2026 requires schools and colleges to take a whole-school approach to safeguarding, including online safety, and to maintain appropriate filtering and monitoring systems with an annual documented review of their effectiveness.

- The Department for Education digital and technology standards set expectations for filtering and monitoring, cyber security, digital leadership and governance, including annual cyber risk assessment, secure user accounts,

anti-malware, firewall protection, backups, incident response and staff awareness.

- The Online Safety Act 2023 places duties on regulated online platforms and search services to reduce illegal content and protect children from harmful and age-inappropriate content. Schools should reflect this in online-safety education, reporting routes and safeguarding discussions with students, parents and carers.

- UK GDPR and the Data Protection Act 2018 require the school to protect personal data, maintain data protection policies and procedures, manage data sharing lawfully, use images and CCTV appropriately, respond to subject access requests and report personal data breaches where required

- Schools should consider risks linked to generative AI, AI-generated images, deepfakes, misinformation, harmful interactions, cyber security incidents and mobile/app-based access when reviewing online safety, filtering, monitoring and curriculum content.

- General Data Protection Regulations 2018 https://www.gov.uk/government/publications/guide-to-the-general-data-protection-regulation
- The Freedom of Information Act 2000 http://www.legislation.gov.uk/ukpga/2000/36/contents

31 Remote Learning

31.1 There is a requirement for then schools to be able to ensure ongoing education for all students under unusual circumstances. Please refer to the Remote Learning Policy for how this is monitored.

32 Associated Documentation & Legislation

- Data Protection Act 2018
- Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Racial and Religious Hatred Act 2006
- Sexual Offences Act 2003

- Communications Act 2003 (Section 127)
- The Computer Misuse Act 1990 (Sections 1 – 3)
- Malicious Communications Act 1988 (Section 1)
- Copyright, Design and Patents Act 1988
- Public Order Act 1986 (Sections 17 – 29)
- Protection of Children Act 1978 (Section 1)
- Obscene Publications Act 1959 and 1964
- Protection from Harassment Act 1997
- Keeping Children Safe in Education 2026
- Online Safety Act 2023
- Department for Education digital and technology standards for filtering and monitoring and cyber security

Document Ref:	Version No:	Summary of Changes:	Author	Release Date:	Approved By:
SC16	1	Launch	Gareth Webb	December 2015	
SC16	2	Review 2016 / 2017	Gareth Webb	November 2016	QSGC
SC16	3	Review	Gareth Webb	December 2016	QSGC
SC16	4	Review 2017 / 2018	Gareth Webb	November 2017	QSGC

SC16	5	Implement KCSiE changes	Laura Willis	October 2018	QSGC
SC16	6	Updated Management Details	Laura Willis	November 2018	QSGC
SC16	7	Review 2019/2020	Laura Willis	November 2019	QSGC
SC16	8	Review 2020 / 2021	Laura Rowe	October 2020	QSGC
SC16	9	Review 2021 / 2022	Laura Rowe	October 2021	QSGC
SC16	10	Review 2022 / 2023	Laura Rowe	October 2022	QSGC
GSC16	11	GLADE Review 2023/2024	Laura Rowe	July 2023	PSC
GSG16	12	GLADE Review 2024/2025	Emma Moore	October 2024	PSC
GSC16	13	Removed all references to 'E-Safety Coordinators'	Laura Rowe	March 2025	PSC

Appendix A – Parent letter

Dear Parent / Carer

ICT including the internet, e-mail, mobile technologies and online resources, have become an important part of learning in our school. We expect all pupils to be safe and responsible when using any ICT. It is essential that pupils are aware of e-safety and know how to stay safe when using any ICT.

Pupils are expected to read and discuss this agreement with their parent or carer and then to sign and follow the terms of the agreement. Any concerns or explanation can be discussed with their class teacher or senior leadership team.
Please return the bottom section of this form to school for filing.

✂ - - -

Appendix B - Acceptable Use Agreement: Pupils – Secondary

- I will only use ICT systems in school, including the internet, e-mail, digital video and mobile technologies for school purposes.
- I will not download or install software on school technologies.
- I will follow the schools ICT security system and not reveal my passwords to anyone and change them regularly.
- I will be responsible for my behaviour when using the Internet. This includes resources I access and the language I use.
- I will not deliberately browse, download, upload or forward material that could be considered offensive or illegal. If I accidentally come across any such material I will report it immediately to my teacher.
- I will not give out any personal information such as name, phone number or address. I will not arrange to meet someone unless this is part of a school project approved by my teacher.
- Images of pupils and/ or staff will only be taken, stored and used for school purposes in line with school policy and not be distributed outside the school network.
- I will ensure that my online activity, both in school and outside school, will not cause my school, the staff, pupils or others distress or bring into disrepute.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the school community.
- I will respect the privacy and ownership of others' work on-line at all times.
- I will not attempt to bypass the internet filtering system.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available to my teachers.

I understand that these rules are designed to keep me safe and that if they are not followed, school sanctions will be applied, and my parent/ carer may be contacted.

Pupil Signature

I agree to follow this code of conduct and to support the safe and secure use of ICT throughout the school

Signature: ……

Date: ……

Appendix C - Acceptable Use Agreement / Code of Conduct: Staff and Visitors

E-SAFETY CODE OF CONDUCTION DECLARATION

In signing this document, I confirm that I have understood the Company E-Safety Code of Conduct which supports the safe and secure use of ICT throughout the school and agree to work in accordance with its requirements.

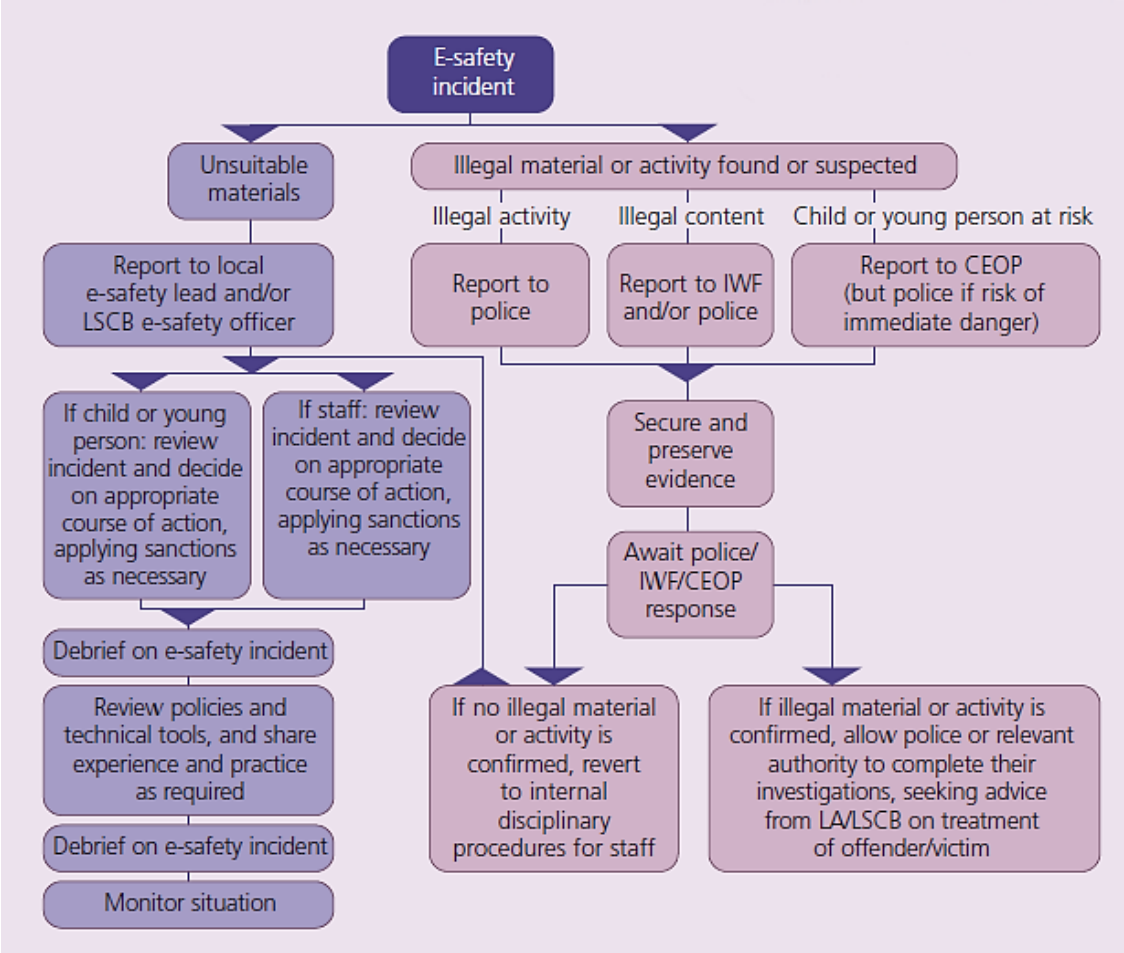
ICT (including data) and the related technologies such as e-mail, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this declaration and adhere at all times to its contents. Any concerns or clarification should be discussed with the Head Teacher or senior leadership team.

- I will only use the school's email, Internet, Intranet, Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number and personal e-mail address, to pupils.
- I will only use the approved, secure e-mail system(s) for any school business.
- I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body.
- I will not install any hardware of software without permission of the Head Teacher
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and/ or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Head teacher.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the school community

- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Head teacher.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will support and promote the school's e-Safety and Data Security policies and help pupils to be safe and responsible in their use of ICT and related technologies.
- I understand this forms part of the terms and conditions set out in my contract of employment.

Worker signature	
Place of work	
Print name	
Date	

Appendix D - Flowcharts for Managing an e-Safety Incident



Source: Becta "Safeguarding Children Online", 2007