Marjory Kinnon School

e-Safety Policy

January 2022

Marjory Kinnon School - e-Safety Policy

1. Introduction

Computing is an essential resource to support learning and teaching and has an important everyday role in children's lives. We therefore need to build the use of Computing/ICT to give them skills to access life-long learning.

Computing covers a wide range of resources. There is constant evolution of computing and technology within society. Currently the wide range of digital technologies children and young people are using both inside and outside of the classroom could include:

- Websites.
- Apps.
- Learning Platforms and Virtual Learning Environments.
- Email and Instant Messaging.
- Social Networking, Blogs and Wikis, Podcasting.
- Video Broadcasting and sharing.
- Music Downloading and downloading.
- Gaming on consoles and PC.
- Mobile/Smart phones with text, video and/or web functionality.
- Other mobile devices with web functionality.

Whilst exciting and beneficial, much technology - particularly web-based resources - is not consistently policed. All need to be aware of the range of risks linked with the use of internet technologies.

At Marjory Kinnon School, we understand the responsibility to educate pupils on e-Safety issues; teaching appropriate behaviours to enable them to remain safe and legal when using the internet and related technologies, in and beyond the classroom.

This Policy and the Acceptable Use Agreements (for all staff, governors, visitors and pupils) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, tablets, webcams, whiteboards, digital video equipment, smartphones, etc.); and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones, camera phones and portable media players, etc.).

Visitors using the school ICT system through desktop or laptop devices (e.g. in-school training) are required to sign Appendix A. Other visitors, who have limited access and use (e.g. Wifi only) will be advised of their requirement to comply with the e-Safety Policy as they log onto the Inventry Visitor Access System.

2. Pupils with Additional Needs

At Marjory Kinnon School we cater for pupils who require additional specialist teaching and differentiated curriculum in order to address learning and communication difficulties. This means that we need to be even more vigilant to address issues of e-Safety at a level that they can understand including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of e-Safety issues.

For our pupils with difficulties in social understanding, careful consideration is given to group interactions when raising awareness of e-Safety. Internet activities are planned, well managed and supervised for these children and young people.

We understand that there is an associated further vulnerability for our pupils when interacting with internet technologies therefore we ensure our practice/safety standards are of very high quality.

3. Roles and Responsibilities

As e-Safety is an important aspect of strategic leadership within the school, the Headteacher and Governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. e-Safety issues at Marjory Kinnon School are dealt with as child protection problems which are addressed by the Designated Safeguarding Lead: Amy Higgins and the e-Safety Officer: Caroline Van Dyk. All members of the school community are made aware of this through staff briefings and Safeguarding noticeboards. The role of the e-Safety leads is to keep abreast of current issues and guidance.

Senior Management and Governors are to be updated by the Headteacher/Safeguarding Team in relation to local and national guidelines and advice.

This Policy, supported by the school's acceptable use agreements for staff, governors, visitors and pupils (appendices), is to protect the interests and safety of the whole school community.

e-Safety skills development for staff

- Staff will receive regular information and training on e-Safety issues as part of the ongoing CPD training.
- New staff will receive the school's Acceptable Use Agreement as part of induction.
- All staff will be made aware of individual safeguarding responsibilities relating to e-Safety and know what to do in the event of misuse of technology (see attached flowchart).
- All staff are to incorporate e-Safety activities and awareness within their curriculum areas.

Managing the school e-Safety messages

- We endeavour to embed e-Safety messages whenever the internet and/or related technologies are used.
- The pupils are taught the programme of study provided by the DfE, each year we begin with the e-Safety topic which also corresponds with our e-Safety Policy. The content is adapted for pupils to allow them to access it.
- e-Safety posters will be prominently displayed. They will be adapted for the range of needs of our pupils.

e-Safety Reporting

It is a responsibility of all staff to report e-Safety incidents. Urgent issues should be notified to the e-Safety Officer immediately via:-

- Hardcopy e-Safety Incident Forms in the Staff Room.
- Online e-Safety Incident Forms on staff laptop/PC desktops.

4. e-Safety in the Curriculum

Computing and online resources are increasingly used across the curriculum. It is therefore essential for e-Safety guidance to be given to the pupils on a regular basis.

- The school provides opportunities in a range of curriculum areas to teach e-Safety.
- Educating pupils on the dangers of technologies encountered outside school is done informally when opportunities arise.
- Pupils are presented with relevant legislation on using the internet and its content. This will be adapted to the pupils' level of understanding.
- Pupils are taught about copyright and data protection and how to use information and content appropriately.
- Pupils will be made aware of the impact of online bullying. Pupils within the curriculum will be educated on forms of cyber bullying and different ways it can occur. This will also include how to seek advice or report problems when using the internet and other related technologies; i.e. parent/carer, teacher/trusted staff member, or an organisation such as ChildLine/CEOP report abuse button.
- Pupils are taught to critically evaluate the validity and trustworthiness of materials and learn good web searching skills.
- Web filtering is controlled by London Grid for Learning (LGfL) which denies access to inappropriate/illegal websites, examples of prohibited content include sites that may be of a sexual, extreme or dangerous nature, reducing the risk of pupils being exposed to content that can cause distress or harm.
- Web browser controls may be used to control access pupils have to sites or apps.

5. Password Security

Password security is essential for staff, particularly as they are able to access and use pupil data. Staff are expected to have secure passwords which are not shared. Pupils/Parents are expected to keep any passwords secret and not to share with others. Staff and pupils will be regularly reminded of the need for password security.

- All users read and sign an Acceptable Use Agreement.
- If you think a password may have been compromised report this to the ICT Team.
- Staff are aware of their individual responsibilities to protect the security and confidentiality of school networks, MIS systems and/or Learning Platform. Individual staff users must also make sure that workstations are not left unattended and are locked.

6. Data Security

The accessing and appropriate use of school data is something that the school takes very seriously. The school follows Becta guidelines and is also GDPR compliant.

- Staff are aware of their responsibility when accessing school data whether in physical hardcopy format or electronic format. Level of access is determined by the Headteacher/Chief Operating Officer and is governed by principles as laid out in the GDPR.
- In August 2018, the school updated its servers to provide staff with a secure remote log in system. This ensures that there is no need for staff to take any data off the school premises. School devices have appropriate secure VPN access which ensure the highest level of security for electronically stored school data.
- All school cloud technologies, including our online progress systems, have the required level of security built in to them.
- Physical data is now kept in two self-contained security storage locations. These records are split between pupil archived records and school business management archive records. Access to these two areas is strictly controlled on the basis of staff having a legitimate and lawful need to access the information being retained.
- The school has moved to a secure 'Follow-Me' queue print system which ensures that printing is only released once the user is physically at the printer/copier device and able to take physical receipt of documents printed. Signage is located at every print/copy location in the school, reminding staff of their obligations around data protection and in particular pupil/staff sensitive information as per the requirements of GDPR.
- There is the facility in the school for secure document disposal via two methods - shredders around the school and secure confidential waste disposal by the Shred-It company.
- The school data is backed up using LGfL's GridStore service to a secure off-site facility where it is fully encrypted.
- Staff are made aware of this through regular training, e-Safety training, notices in the Staff Room and via school policies.

7. Managing the Internet

The internet is an open communication medium. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource but also a potential risk to young and vulnerable people. Whenever any inappropriate use is detected it will be followed up.

- The school maintains that pupils will have supervised access to internet resources (where reasonable) through the school's fixed and mobile internet technology.
- Staff will preview any recommended sites before use.
- Raw image searches are discouraged when working with pupils.
- 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.

Infrastructure

School internet access is controlled by LGfL web filtering (WebScreen 2.0 incorporating Netsweeper and Fortinet technologies), which denies access to inappropriate websites including pornography, radicalisation and extremist views. User activity is also monitored by the Securus online safety solution for schools.

- Marjory Kinnon School is aware of its responsibility when monitoring staff communication under current legislation and takes into account: Data Protection Act 1998 (superseded in 2018), The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000, Human Rights Act 1998.
- Staff are aware that to ensure the highest possible safeguarding practices and professional standards, school based email, internet activity and computer usage is constantly monitored and explored further if required.
- If staff or pupils discover an unsuitable site, the screen must be switched off/closed and the incident reported immediately to the e-Safety Officer. The offending URL will be reported to the LA and LGfL.
- Sophos Anti-Virus protection is set to automatically update on all school machines including staff machines with access to the internet.

- Pupils and staff are not permitted to download executable programs or files on school based technologies without seeking prior permission.
- If there are any issues related to viruses or anti-virus software, the ICT Team should be informed immediately.

8. Managing Other Web 2 Technologies

Web 2, including social networking sites, if used responsibly within education, can provide easy to use, creative, collaborative and free facilities. 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 staff acting on behalf of our pupils to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.

- We endeavour to deny access to social networking features of any sites to pupils within school, unless permission is given and is part of a teacher-led educational activity.
- All pupils, and in loco parentis, staff are advised to be cautious about the information given by others on sites, for example users not being who they say they are.
- Except for official school channels where permissions have been given - there is no placing of pupil images (or details within images that could give background details) on such sites.
- No pupil's personal details are given out on such sites which may identify them or where they are.
- Our staff, who monitor all internet activity, are to report any incidents.
- Staff understand it is highly inappropriate to use open social networking features within sites and public chat room facilities with pupils. They are expected to use the tools within the resources provided.

9. Mobile Technologies

Emerging technologies may offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Existing mobile technologies such as tablets, portable media players, PDAs, gaming devices, mobile and smartphones are familiar to children outside of school too. There is risk and misuse associated with communication and internet use therefore 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:

Mobile devices (including phones)

- The school allows staff to bring in personal mobile phones and devices for their own use.
- Staff should where possible use school facilities to contact parents/carers. If no device is accessible and staff have permission from SLT, a personal device may be used but staff may not reveal personal information such as phone number to pupils or parent/carers by using their personal device. Personal mobile technology may be used, for educational purposes, as mutually agreed with the Headteacher.
- The school is not responsible for the loss, damage or theft of any personal mobile device whilst on school premises.
- The sending of inappropriate messages through electronic devices 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.
- Capturing images and video is not allowed by students / staff unless on school equipment and for educational purposes.
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.
- Where the school provides mobile technologies such as phones, laptops and PDAs for offsite visits and trips, only these devices should be used.

10. Managing Email

The use of email within school is an essential means of communication. In the context of school, email 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 our pupils need 1:1 support, guidance and approval IF email is to be used on their behalf.

- Staff have a school LGfL account for all school business to minimise risk of receiving unsolicited or malicious emails and avoid personal profile information being revealed.
- 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. This should be the account that is used for all school business.

- Under no circumstances should staff contact pupils, parents or conduct any school business using personal email addresses.
- Email sent to an external organisation should be written carefully before sending, in the same way as a letter written on school headed paper.
- Pupils may only use school approved accounts (LGfL LondonStaffMail) on the school system and only under direct teacher supervision for educational purposes.
- All email users are to adhere to the accepted rules of network etiquette (netiquette) particularly in relation to use of appropriate language and not revealing any personal details about themselves or others, or arrange to meet anyone without specific permission.
- Pupils, or staff monitoring email use, must immediately report any offensive message and keep the offending message(s) as evidence.
- Staff must inform the e-Safety Officer if they receive an offensive email.
- Formal pupil information sent by email between schools and the Local Authority is encrypted.

11. Safe Use of Images & Film

11.1 Taking of Images & 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 pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment.
- Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, this includes when on field trips.
- Pupils are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of the others, this includes when on field trips.
- Photos and videos are used as a means of assessment at Marjory Kinnon School and it is the responsibility of all staff to ensure these images are safely secured.

11.2 Consent of Adults Who Work at the School

- Permission to use images of all staff who work at the school is sought on a regular basis. Staff can refuse permission at any time.

11.3 Publishing Pupils' Images & Work

On a child's entry to the school, all parents/guardians will be asked to give permission to use their child's photos in the following ways:

- On the school website/on line.
- In the school prospectus and/or publications that may be produced for school promotion.
- Recorded/ transmitted on a video or webcam.
- In display material that may be used in the school's communal areas.
- In display material that may be used in external areas, e.g. exhibition promoting the school.
- General media appearances, e.g. local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically).
- 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. Parents/carers may withdraw permission, in writing, at any time. Pupils' names will not be published alongside their image and vice versa. Email and postal addresses of pupils will not be published. Before posting student work on the internet, a check needs to be made to ensure that permission has been given for work to be displayed. Video is only streamed from the service set to private. Only previously authorised and trained members of staff have authority to upload to the public website.

11.4 Storage of Images

- Images/films of children are to only be stored on the school's network and online storage that has the required level of data protection in place.
- Rights of access to raw images are restricted to the staff and pupils within the confines of the school network. The school may publish photos on an individual basis. Adhering to the policies on staff and parental consent.
- Staff have the responsibility of deleting images when no longer required.

11.5 Webcams & CCTV

- The school uses CCTV for security and safety. This is only accessed by authorised staff. Notification of CCTV use is displayed at the front of the school.
- We do not use publicly accessible webcams in school other than for special specifically vetted and authorised projects. Misuse of the webcam by any member of the school community will result in sanctions (as listed under the 'inappropriate materials' section of this document).
- In the case of remote learning using a webcam, it is the responsibility of the parent/carer to make sure they either activate or deactivate the devices camera to their preferred setting. If the webcam is activated in a video call it may be visible by other computers. Parents and carers acknowledge this and accept this as part of using the service.
- If webcams are used for meetings it is necessary to alert all present if recording is going to be used and should adhere to agreed photo permissions.
- Any games console connected to a camera may not be connected to the internet at the same time and may only be used under supervision of a staff member.
- Where webcams are present within classrooms these may not be used as mentioned for any CCTV purpose and can only be activated by staff present in the room.

11.6 Video Conferencing

- Permission is sought from parents and carers if their children are involved in video conferences.
- When in school all pupils are supervised by a member of staff if video conferencing.
- Approval from the Headteacher is sought prior to all pupil video conferences within school with a non-member of staff.
- No part of any video conference is recorded in any medium without the written, verbal or visual consent of those taking part.

11.7 Visitors to Marjory Kinnon School

- All persons who enter Marjory Kinnon School (staff, parents or visitors) who seek to use ICT systems are bound by the Acceptable Use Policy. This Policy clearly outlines the use of recordings.
- No images of pupils are to be uploaded to social networking sites that would breach agreed photo permissions.

12. Misuse & Infringements

12.1 Incident Reporting

- Incidents relating to e-Safety should be reported to the e-Safety Officer or Headteacher. Incidents should be logged (see Incident Log in Appendix D) and process should be followed (see Flowchart in Appendix E).

12.2 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 Officer.
- Deliberate access to inappropriate materials by anyone will lead to the incident being logged by the e-Safety Officer and, depending on the seriousness of the offence, investigation by the Headteacher and Local Authority and immediate suspension, possibly leading to dismissal and involvement of police for very serious offences.

13. Equal Opportunities

The school endeavours to create a consistent message with parents for all pupils and this in turn should aid establishment and future development of the school's e-Safety rules.

14. Parental Involvement

We believe that it is essential for parents/carers to be fully involved with promoting e-Safety both in and outside of school. We aim to regularly consult and discuss e-Safety with parents/carers and seek to promote a wide understanding of the benefits related to ICT and associated risks.

- Parents/carers and pupils are to be actively encouraged to contribute to adjustments or reviews of the school e-Safety Policy.
- Parents/carers are asked to read through and sign an Acceptable Use Agreement on behalf of their child on admission to school.
- Parents/carers are required to make a decision as to whether they consent to images of their child being taken/used in the public domain (e.g. on the school website).
- Parents/carers are required to decide to activate or deactivate webcams or microphones when connecting to remote video conferencing.
- The school disseminates information to parents relating to e-Safety where appropriate in the form of:

- Information meetings
- Posters
- Website/Learning Platform training and postings
- Newsletter items

- We seek verbal agreement from parents: “I agree that I shall not take any photographs or images at school events”.
- Parents are requested NOT to video school performances. Videos are captured ONLY by school staff.

15. Current Legislation

15.1 Acts Relating to Monitoring of Staff Email

Data Protection Act 1998 (superseded in 2018, the Act supplements EU GDPR)

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

A number of the requirements of the Data Protection Act 2018 will come into play whenever an employer wishes to monitor workers. The Act does not prevent an employer from monitoring workers, but such monitoring must be done in a way which is consistent with the Act. Employers – especially in the public sector – must also bear in mind Article 8 of the European Convention on Human Rights which creates a right to respect for private and family life and for correspondence.

The aim of the Information Commissioner’s Office (ICO) Employment Practices Code is intended to help employers comply with the Data Protection Act and to encourage them to adopt good practice. The code aims to strike a balance between the legitimate expectations of workers that personal information about them will be handled properly and the legitimate interests of employers in deciding how best, within the law, to run their own businesses. It does not impose new legal obligations.

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

15.2 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 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).
- Gain 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 the 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 & 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.

Counter Terrorism & Security Act 2015

In July 2015 the UK Government published the following document with advice for schools about how the new law impacts on schools' duty under the 'Prevent' scheme. This was aimed at safeguarding children against radicalisation. A school-specific section can be found on pages 10-13.

https://www.gov.uk/government/publications/protecting-children-from-radicalisation-the-prevent-duty.

16. Policy Review

There will be an on-going opportunity for staff to discuss with the e-Safety Officer any issue of e-Safety that concerns them.

This Policy will be reviewed regularly and consideration given to the implications for future whole school development planning.

The Policy will be amended if new technologies are adopted or Central Government change the orders or guidance in any way.

Approved by the Safeguarding Committee: January 2022

APPENDIX A: Acceptable Use of IT Agreement (Visitors)

Acceptable Use of IT Agreement (Visitors)

This Agreement supplements the e-Safety Policy alongside the guidance notes for Acceptable Use of Internet & Technologies that users must comply with. Visitors are recommended to ensure they are familiar with, and understand the content of these policies.
Any concerns or clarification should be discussed with Caroline Van Dyk, e-Safety Officer.

- You are advised that all work undertaken using the Internet and Wi-Fi service is monitored and logged, not only for this purpose but also to allow monitoring of service provision.
- By using Wi-Fi and Internet services you are bound to the relevant UK law, including the Data Protection Act 1998; Computer Misuse Act 1990; Copyright, etc. and Trade Marks (Offences and Enforcement) Act 2002, and agree to abide by it. It is your responsibility to familiarise yourself with all Statutory requirements.
- In particular**, <u>you must not</u>** and by using the service you **<u>agree not to</u>:**
  - Access network services in such a way as to deny reasonable access to the network for other users, for example, by excessive use of network bandwidth. This could include the use of FTP servers, file-sharing software and video streaming
  - Download any images, text, sound or other material that is in breach of copyright. The School accepts no responsibility for any breaches that may occur.
  - Deliberately visit, view or download any material from any website containing pornographic, abusive, racist, violent or illegal material or material which is offensive in any way whatsoever. The Schools decision as to which websites fall into these categories is final.
  - Upload or make available to others any material that is offensive, obscene, indecent, or which infringes the copyright of another person (e.g. images, MP3 and other audio and video files).
  - Use School printing services without prior approval from the school.
  - Use the Internet for any illegal activity or gambling.
  - Use the Internet to harass, cause annoyance, inconvenience or anxiety to others.
  - Access, or attempt to gain access to, computer systems, data or resources to which they are not authorised, such as connecting to other user's resources.
  - By using the service you agree to respect the Privacy of others.
  - Attempt to gain unauthorised access to restricted part of the network, or attempt to undermine the integrity or security of any computer systems or network. You, the user, are responsible for any damage caused to the computer equipment arising out of any wilful act or negligent misuse.

Breach of the above will lead to users being banned from using the service and may result in prosecution.

The School reserve the right to update or modify the above terms at any time without prior notice. Your use of the Service following any such change constitutes your agreement to follow and be bound by these terms as modified.

Disclaimer

- **Service provided "as is".** This Service provides access to the Internet on an "as is" basis with all risks inherent in such access.
- **Service provided "as available".** The Service is provided on an "as available" basis without warranties of any kind, either express or implied.

- **Indemnity.** The school assumes no responsibility for damages, direct or indirect from its connections to the internet, nor for the accuracy and effectiveness of any installed filter. The school cannot be held liable for any information that may be lost, damaged, stolen or unavailable due to technical or other difficulties.
- The school is not responsible for the configuration of any personal equipment or changes to these resulting from connection to the School's network. It is the sole responsibility of users to provide anti-virus protection, personal firewall protection and to configure their device's (laptop / PDA (Personal digital assistant) or other equipment) settings to provide the appropriate security settings to control access from other wireless devices within the range of the school's Wi-Fi service and the Internet itself.

User Signature			
I agree to follow this Agreement / Guidance for Acceptable Use of Internet & Technologies / e-Safety Policy			
Visitor Name: (Print)			
Signature:		Date:	
Job Title/Company:			

e-Safety
Logged by the e-Safety Officer: *(Signature / Date)*

APPENDIX B: Acceptable Use of IT Agreement (Staff/Governors)

Acceptable Use of IT Agreement (Staff/Governors)

This Agreement forms part of the e-Safety Policy alongside the guidance notes for Acceptable Use of Internet & Technologies. It 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 agreement and adhere at all times to its contents.
This is an extraction from the e-Safety Policy and the Guidance notes.
Any concerns or clarification should be discussed with Caroline Van Dyk, e-Safety Officer.

- I have read the guidance notes for Acceptable Use of Internet & Technologies and understand that both the agreement and guidance notes form part of the e-Safety Policy.
- I understand that the school uses Securus online safety solution for schools, and that if I choose to use a school device off site for personal use that the Securus system will scan my laptop and if it detects inappropriate websites including pornography, radicalisation, extremist views that it will save a screen shot that is then monitored by the e-Safety Officer.
- I agree to bring in my school device for maintenance and Securus screening when requested.
- I will only use the school's hardware or software for professional purposes or for uses deemed 'reasonable' by the Headteacher 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 email address, to pupils or parents.
- I will only use software approved by the school for communications with pupils/parents.
- I am aware that communicating with pupils via private email/ SMS and social networking sites may be considered a disciplinary matter in this school.
- I will ensure that personal data (such as data held on SIMS) is 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 Headteacher or Governing Body.
- I will not handle sensitive data whilst working from home or remotely (or in a public space) on a device without adequate protection; or whilst using a public/unsecured WiFi connection without Headteacher authorisation.
- I will not alter or install any hardware of software without the permission of the ICT Team.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory and **understand that to do so may constitute a disciplinary offence and in some cases a criminal offence.**
- 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 or cloud-based services authorised by the school without the permission of the parent/carer or member of staff) for their individual files/images) or the Headteacher for overarching permission.
- 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 policy and help pupils to be safe and responsible in their use of ICT and related technologies.
- By activating (for work purposes) a device's webcam, I am agreeing for my image to be visible (temporarily overriding any other agreement on photo permissions). I am aware that if I do not want my photo permissions to change, I need to disable my device's webcam and contact my DHT to inform them.

User Signature			
I agree to follow this Agreement / Guidance for Acceptable Use of Internet & Technologies / e-Safety Policy			
Full Name: (printed)			
Signature:		Date:	
Job Title:			

e-Safety
Logged by the e-Safety Officer: *(Signature / Date)*

APPENDIX C: Use of the Internet by Pupils

Marjory Kinnon School

USE OF THE INTERNET BY PUPILS

We use the school computers and Internet connection for learning. These rules will help us to be fair to others and keep everyone safe. We would like you to sign below to record that you are aware of the school rules regarding use of the internet.

SCHOOL INTERNET RULES
❖ I will stop watching a video or playing a game if an adult thinks it is inappropriate.
❖ On a network, I will use only my own login and password, which I will keep secret.
❖ I will not look at or delete other people's files.
❖ I will not bring memory sticks (USB sticks) into school without permission.
❖ I will only e-mail people I know, or my teacher has approved.
❖ The messages I send will be polite and sensible.
❖ When sending an e-mail, I will not give my home address or phone number, or arrange to meet someone.
❖ I will ask for permission before opening an e-mail or an e-mail attachment sent by someone I do not know.
❖ I will not use Internet chat.
❖ If I see anything I am unhappy with or I receive messages, I do not like; I will tell a teacher immediately.
❖ I know that the school may check my computer files and may monitor the Internet sites I visit.
❖ I understand that if I deliberately break these rules I could be stopped from using the Internet or computers.

I agree for staff to operate these procedures in school

PUPIL INFORMATION			
Child's Surname		Forename	

Parent/Guardian Name			
Signature		Date	

School Use Only
Seen and entered by Pupil Information Manager: *(signature and date)*

For pupils younger than 16 years - this form must be completed by the parent or legal guardian. Pupils over 16 who are able to provide informed consent - can complete this form themselves, having discussed with their parent / guardian if under 18. For any pupil who does not have the capacity to provide informed consent - this form must be completed by the parent or legal guardian.

APPENDIX D: Incident Log

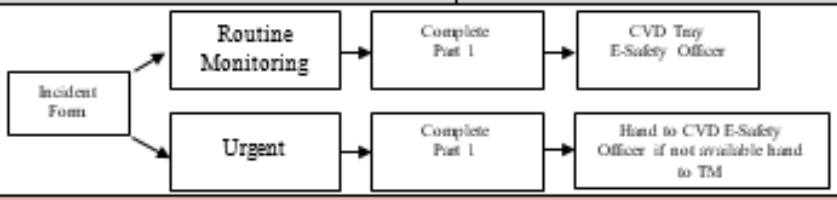
The log is maintained by the e-Safety Officer.

Marjory Kinnon School - E-Safety Incident Log														
All paper forms and online forms are stored in the E-Safety Folder with a Ref No. All serious incidents are logged on My Concern														
Ref No	Academic Year	Incident Date	Forename	Surname	Yr Grp	Gender	Person reporting	Date Reported	How was it reported?	Location of Incident	Incident at Home or School?	Incident accidental or deliberate?	Classed as	Logged on My Concern
	2018-19				6	M			Online Form			accidental	Routine Monitoring	no
					10	F			Paper Form			deliberate	Urgent	yes

APPENDIX E: e-Safety Incident Form

MARJORY KINNON SCHOOL
E-SAFETY INCIDENT FORM – PART 1

Routine monitoring ☐	Urgent ☐



PART A – ABOUT THE PERSON *To be completed by the responsible member of staff*

INCIDENT COMES FROM CHILD				INCIDENT COMES FROM ADULT			
Child's name:				Adult's name:			
Class:				Job title:			
Date of birth:	/ /	Gender:	M / F	Date of birth:	/ /	Gender:	M / F
If visitor, home address and telephone No:							

PART B – ABOUT THE INCIDENT *To be completed by the responsible member of staff*

Date of incident:		Time:	
Location of incident:			
Person reporting incident:		Date of reporting:	/ /
Who was it reported to:		Person completing the form:	
Was the incident due to accidental access?	Yes ☐ No ☐		
Was the incident due to deliberate access?	Yes ☐ No ☐		

Did the incident involve material being:			
created	Yes ☐ No ☐	viewed	Yes ☐ No ☐
printed	Yes ☐ No ☐	shown to others	Yes ☐ No ☐
transmitted to others	Yes ☐ No ☐	distributed	Yes ☐ No ☐

Nature of the incident:			
harassment	Yes ☐ No ☐	cyberbullying	Yes ☐ No ☐
grooming	Yes ☐ No ☐	offensive language typed	Yes ☐ No ☐
racist, sexist, homophobic religious hate material	Yes ☐ No ☐	deliberately bypassing security or access	Yes ☐ No ☐
hacking or virus propagation	Yes ☐ No ☐	on-line gambling	Yes ☐ No ☐
drug making material	Yes ☐ No ☐	bomb making material	Yes ☐ No ☐
Terrorist material	Yes ☐ No ☐	breach of acceptable use policy	Yes ☐ No ☐
child abuse images / soft core pornographic material /illegal hard core pornographic material	Yes ☐ No ☐	Other (please specify)	

Full description of the incident: (please continue on a separate sheet if needed)

APPENDIX F: Flowchart for Misuse/Infringements