Marjory Kinnon School

Online Safety Policy

January 2023

Marjory Kinnon School – Online Safety Policy

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors.
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones').
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- Content – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.
- Contact – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
- Conduct – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying.
- Commerce – risks such as online gambling, inappropriate advertising, phishing and/or financial scam.

2. Legislation & Guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools.
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff.

- Relationships and sex education.
- Searching, screening and confiscation.

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

For further legislative guidance please see Appendix E.

3. 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.).

4. 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.

5. Roles & Responsibilities

5.1 The Governing Body

The Governing Body has overall responsibility for monitoring this Policy and holding the Headteacher to account for its implementation.

The Governing Body will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the Designated Safeguarding Lead (DSL).

The Governor who oversees online safety is: Paul Goulden.

All governors will:

- Ensure that they have read and understand this Policy.
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (Appendix B).
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with SEND because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable.

5.2 The Headteacher

The Headteacher is responsible for ensuring that staff understand this Policy, and that it is being implemented consistently throughout the school.

5.3 The Designated Safeguarding Lead & Deputy Designated Safeguarding Lead

Details of the school's DSL and DDSL are set out in our Child Protection & Safeguarding Policy as well as relevant job descriptions.

The DDSL (Ali Sedaghat) takes lead responsibility for online safety in school, in particular:

- Supporting the Headteacher in ensuring that staff understand this Policy and that it is being implemented consistently throughout the school.

- Working with the Headteacher, ICT Team and other staff, as necessary, to address any online safety issues or incidents.
- Managing all online safety issues and incidents in line with the school Child Protection & Safeguarding Policy.
- Ensuring that any online safety incidents are logged (see Appendix D) and dealt with appropriately in line with this Policy.
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school Behaviour Policy.
- Updating and delivering staff training on online safety (Appendix C contains a self-audit for staff on online safety training needs).
- Liaising with other agencies and/or external services if necessary.
- Providing regular reports on online safety in school to the Headteacher and/or Governing Body.

This list is not intended to be exhaustive.

5.4 The ICT Team

The ICT team is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material.
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly.
- Conducting a full security check and monitoring the school's ICT systems on a regular basis.
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.

This list is not intended to be exhaustive.

5.5 All Staff & Volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this Policy.
- Implementing this Policy consistently.
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (Appendix B), and ensuring that pupils follow the school's terms on acceptable use (Appendix A).
- Working with the DSL to ensure that any online safety incidents are logged (see Appendix D) and dealt with appropriately in line with this Policy.
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school Behaviour Policy.
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'.

This list is not intended to be exhaustive.

5.6 Parents

Parents are expected to:

- Notify a member of staff or the Headteacher of any concerns or queries regarding this Policy.
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (Appendices A and B).
- Parents can seek further guidance on keeping children safe online from the following organisations and websites:
- What are the issues? – UK Safer Internet Centre
- Hot topics – Childnet International
- Parent resource sheet – Childnet International
- Healthy relationships – Disrespect Nobody

5.7 Visitors & Members of the Community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (Appendix B).

6. Managing the internet and online activity

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 Online 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.

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.

7. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum:

The text below is taken from the National Curriculum computing programmes of study. It is also taken from the guidance on relationships education, relationships and sex education (RSE) and health education.

All schools have to teach:

- Relationships education and health education in primary schools.
- Relationships and sex education and health education in secondary schools.

In Key Stage 1, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private.
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies.

Pupils in Key Stage 2 will be taught to:

- Use technology safely, respectfully and responsibly.
- Recognise acceptable and unacceptable behaviour.
- Identify a range of ways to report concerns about content and contact.

By the end of primary school, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not.
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous.
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them.
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met.
- How information and data is shared and used online.
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context).
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know.

In Key Stage 3, pupils will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy.
- Recognise inappropriate content, contact and conduct, and know how to report concerns.

Pupils in Key Stage 4 will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity.
- How to report a range of concerns.

By the end of secondary school, pupils will know:

- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online.
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online.
- Not to provide material to others that they would not want shared further and not to share personal material which is sent to them.
- What to do and where to get support to report material or manage issues online
- The impact of viewing harmful content.
- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners.
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including jail.
- How information and data is generated, collected, shared and used online.
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours.
- How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online).

The safe use of social media and the internet will also be covered in other subjects where relevant.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

Full coverage of aspects of online safety can be found in the Annual Audit Appendix G

8. Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website or virtual learning environment (VLE). This policy will also be shared with parents.

Online safety will also be covered during parents' evenings if there are any concerns raised.

We will also provide regular parental workshops on different topics relating to online safety.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the Headteacher and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the Headteacher.

9. 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.

10. Cyber Bullying

10.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school Behaviour Policy.)

10.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyber-bullying with their tutor groups.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate. (See Appendix G).

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

The school also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school Behaviour Policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

10.3 Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police*

* Staff may also confiscate devices for evidence to hand to the police, if a pupil discloses that they are being abused and that this abuse includes an online element.

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on screening, searching and confiscation.
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people.
- The school's COVID-19 risk assessment.

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

11. Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (Appendices A-C). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements in Appendices A, and B.

12. Pupils using mobile devices in school

Pupils may bring mobile devices into school, but are not permitted to use them during:

- Lessons.
- Tutor group time.
- Clubs before or after school, or any other activities organised by the school.

Any use of mobile devices in school by pupils must be in line with the acceptable use agreement.

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school Behaviour Policy, which may result in the confiscation of their device.

13. Staff using mobile technology in school

Staff may bring mobile devices into school, but are not permitted to use them during:

- Lessons.
- Tutor group time.
- Clubs before or after school, or any other activities organised by the school.
- In areas of the building where pupils are present.

Any use of mobile devices in school by staff must be in line with the acceptable use agreement this includes when and where they might be used.

Any breach of the acceptable use agreement by a member of staff may trigger disciplinary action in line with the code of conduct.

For more detail see Appendix F.

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.

14. Misuse & Infringements

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol).
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device.
- Making sure the device locks if left inactive for a period of time.
- Not sharing the device among family or friends.
- Installing anti-virus and anti-spyware software.
- Keeping operating systems up to date – always install the latest updates.

Staff members must not use the device in any way which would violate the school's terms of acceptable use, as set out in Appendix B.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from their line manager.

15. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on behaviour and ICT and internet acceptable use. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents, which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

For the full process see Appendix H flow chart.

15.1 Incident Reporting

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

15.2 Inappropriate Material

All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the Online Safety Officer.

Deliberate access to inappropriate materials by anyone will lead to the incident being logged by the Online 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.

16. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation. All new staff will be required to read and sign our Guidance for Acceptable use of ICT and Technologies (see Appendix B).

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse.
- Children can abuse their peers online through:
    - Abusive, harassing, and misogynistic messages.
    - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups.
    - Sharing of abusive images and pornography, to those who don't want to receive such content.
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element.

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse.
- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh the risks up.
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term.

The nominated safeguarding lead will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our Safeguarding & Child Protection Policy.

17. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety.

An incident report log can be found in Appendix D.

This policy will be reviewed every year by the Headteacher. At every review, the policy will be shared with the governing board. The review will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

18. Links with other policies

This Online Safety Policy is linked to our:

- Safeguarding & Child Protection Policy.
- Behaviour Policy.
- Disciplinary Policy & Procedure.
- Professional Code of Conduct.
- Data Protection Policy and Privacy Notices.
- Complaints Procedure
- Guidance on the Acceptable Use of Internet & Technologies.

APPENDIX A: Pupil Acceptable Use Agreement (Pupils and Parents/Carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS	
Name of pupil:	**Name of parent/carer**

When I use the school's ICT systems (like computers) and get onto the internet in school I will:
• Ask a teacher or adult if I can do so before using them
• Only use websites that a teacher or adult has told me or allowed me to use
• Tell my teacher immediately if:
  ○ I click on a website by mistake
  ○ I receive messages from people I don't know
  ○ I find anything that may upset or harm me or my friends
• Use school computers for school work only
• I will stop watching a video or playing a game if my teacher or TA thinks it is unsuitable
• I will not look at or delete other peoples files
• I will not use internet chat
• Be kind to others and not upset or be rude to them, the messages I send will be polite and sensible.
• Look after the school ICT equipment and tell a teacher straight away if something is broken or not working properly
• Only use the username and password I have been given
• Try my hardest to remember my username and password
• Never share my password with anyone, including my friends.
• Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer
• Save my work on the school network , I will not bring USB or storage devices into school
• Check with my teacher before I print anything
• Log off or shut down a computer when I have finished using it
 	
I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.	

Signed (pupil):	**Date:**
Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

APPENDIX B: Acceptable Use Agreement (Staff/Governors/Volunteers/Visitors)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS,VOLUNTEERS AND VISITORS
Name of staff member/governor/volunteer/visitor:

This Agreement forms part of the Online 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.

Any concerns or clarification should be discussed with Ali Sedaghat Online 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 Online 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 Online 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, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)
- I will not browse, download, upload or distribute any material that could be considered 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.

Signed: (Staff Member/Governor/Volunteer/Visitor)	**Date:**

APPENDIX C: Online Safety Training Needs – Self Audit for Staff

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	**Date**:
Question	**Yes/No (add comments if necessary)**
Do you know the name of the person who has lead responsibility for online safety in school?	
Are you aware of the ways pupils can abuse their peers online?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	

APPENDIX D: Online Safety Incident Report Log

ONLINE SAFETY INCIDENT LOG				
Date	**Where the incident took place**	**Description of the incident**	**Action taken**	**Name and signature of staff member recording the incident**

APPENDIX E: Extended legislative guidance

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.

Freedom of Information Act 2000
The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

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

This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of "higher law", affecting all other laws. In the school context, human rights to be aware of include:

- The right to a fair trial
- The right to respect for private and family life, home and correspondence
- Freedom of thought, conscience and religion
- Freedom of expression
- Freedom of assembly
- Prohibition of discrimination
- The right to education

These rights are not absolute. The school is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

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.

Communications Act 2003

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.

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.

Trade Marks Act 1994

This provides protection for Registered Trade Marks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trade Marks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

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.

Telecommunications Act 1984

It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

Criminal Justice & Public Order Act 1994

This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they:

- Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or

Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress

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

The Education and Inspections Act 2006

Empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students/pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

The Education and Inspections Act 2011

Extended the powers included in the 2006 Act and gave permission for Headteachers (and nominated staff) to search for electronic devices. It also provides powers to search for data on those devices and to delete data.

See DfE guidance - http://www.education.gov.uk/schools/pupilsupport/behaviour/behaviourpolicies/f0076897/screening-searching-and-confiscation)

The Protection of Freedoms Act 2012

Requires schools to seek permission from a parent/carer to use Biometric systems.

The School Information Regulations 2012

Requires schools to publish certain information on its website:

https://www.gov.uk/guidance/what-maintained-schools-must-publish-online

Serious Crime Act 2015

Introduced new offence of sexual communication with a child. Also created new offences and orders around gang crime (including CSE).

Criminal Justice and Courts Act 2015

Revenge porn – as it is now commonly known – involves the distribution of private and personal explicit images or video footage of an individual without their consent, with the intention of causing them embarrassment and distress. Often revenge porn is used maliciously to shame ex-partners. Revenge porn was made a specific offence in the Criminal Justice and Courts Act 2015. The Act specifies that if you are accused of revenge porn and found guilty of the criminal offence, you could be prosecuted and face a sentence of up to two years in prison.

For further guidance or support please contact the Revenge Porn Helpline.

Appendix F: Use of mobile devices in school

The school has provided technical solutions for the safe use of mobile technology for school devices/personal devices (delete/amend as appropriate):

- All school devices are controlled.
- Appropriate access control is applied to all mobile devices according to the requirements of the user (e.g Internet only access, network access allowed, shared folder network access).
- The school/academy has addressed broadband performance and capacity to ensure that core educational and administrative activities are not negatively affected by the increase in the number of connected devices.
- For all mobile technologies, filtering will be applied to the internet connection and attempts to bypass this are not permitted.
- Appropriate exit processes are implemented for devices no longer used at a school/academy location or by an authorised user.

When personal devices are permitted:

- Personal devices are brought into the school entirely at the risk of the owner and the decision to bring the device in to the school/academy lies with the user (and their parents/carers) as does the liability for any loss or damage resulting from the use of the device in school.
- The school accepts no responsibility or liability in respect of lost, stolen or damaged devices while at school or on activities organised or undertaken by the school (the school recommends insurance is purchased to cover that device whilst out of the home).
- The school accepts no responsibility for any malfunction of a device due to changes made to the device while on the school network or whilst resolving any connectivity issues.
- The school recommends that the devices are made easily identifiable and have a protective case to help secure them as the devices are moved around the school. Pass-codes or PINs should be set on personal devices to aid security.
- The school is not responsible for the day to day maintenance or upkeep of the users personal device such as the charging of any device, the installation of software updates or the resolution of hardware issues.

Users are expected to act responsibly, safely and respectfully in line with current acceptable use agreements, in addition;

- Devices may not be used in tests or exams.
- Visitors should be provided with information about how and when they are permitted to use mobile technology in line with local safeguarding arrangements.
- Users are responsible for keeping their device up to date through software, security and app updates. The device is virus protected and should not be capable of passing on infections to the network.
- Users are responsible for charging their own devices and for protecting and looking after their devices while in the school.
- Devices must be in silent mode on the school/academy site and on school buses.
- School devices are provided to support learning. It is expected that pupils/students will bring devices to the school as required.
- Confiscation and searching (England) - the school/academy has the right to take, examine and search any device that is suspected of unauthorised use, either technical or inappropriate.
- The changing of settings (exceptions include personal settings such as font size, brightness, etc…) that would stop the device working as it was originally set up and intended to work is not permitted.
- The software/apps originally installed by the school must remain on the school owned device in usable condition and be easily accessible at all times. From time to time the academy may add software applications for use in a particular lesson. Periodic checks of devices will be made to ensure that users have not removed required apps.
- The school will ensure that devices contain the necessary apps for school work. Apps added by the school will remain the property of the school and will not be accessible to students/pupils on authorised devices once they leave the school roll. Any apps bought by the user on their own account will remain theirs.
- Users should be mindful of the age limits for app purchases and use and should ensure they read the terms and conditions before use.
- Users must only photograph people with their permission. Users must only take pictures or videos that are required for a task or activity. All unnecessary images or videos will be deleted immediately.
- Devices may only be used in lessons in accordance with teacher direction.

- Staff owned devices should not be used for personal purposes during teaching sessions, unless in exceptional circumstances.
- Printing from personal devices will not be possible.

Appendix G: Annual Audit for Online safety

Online Safety – Coverage in PSHE & Computing Annual Audit (March 2022)			
Topics	Year Groups	Content	Number of Hours
Pornography	8	Recognising the risks associated with internet use. Understanding how online activities can expose you and others to risks.	1¼
	10	Understanding the role of sex in the media and its impact on sexuality – including pornography.	½
Fake News	UKS2	Knowing how to be a discerning consumer of information online understanding that information, including that from search engines, is ranked, selected and targeted.	1
	7	Knowing that media portrayal of relationships may not reflect real life. Understanding how to determine whether other children, adults or sources of information are trustworthy.	2
	9	Knowing what constitutes the media. Recognising how the media portrays young people. Understanding how the media portray body image.	2
	10	Identifying, evaluating and independently accessing reliable sources of information, advice and support for all aspects of physical or mental health (including sexual health services). Knowing that the media portrayal of relationships may not reflect real life. Understanding how to determine whether other children, adults or sources of information are trustworthy.	3
	11	Understanding how the media portray body image. Recognizing and managing feelings about, and influences on, their body image including the media's portrayal of idealised and artificial body shapes.	1
Racism	LKS2	Understanding the term 'diversity' and appreciate diversity within school. Recognising and challenging stereotyping and discrimination. Knowing and understanding the terms 'discrimination' and 'stereotype'.	2
	UKS2	Learning about racial discrimination and its impact on societies, past and present.	1
	8	Awareness of the similarities, differences and diversity among people of different ethnicity and culture. Recognising more complex forms of bullying including prejudicial bullying. Understanding the impact of stereotyping, prejudice and discrimination on individuals and communities. Knowing how to respond appropriately to prejudice and discrimination. Knowing how to seek support for victims of stereotyping, prejudice or discrimination.	7

	10	Knowing about the unacceptability of all form of discrimination and how to challenge it; prejudice and bigotry in the wider community including the workplace.	1
Misogyny and Misandry	8	Language and behaviours (types of bullying and discrimination) To become aware of the similarities, differences and diversity among people of different ethnicity, culture, ability, disability, sex, gender identity, age and sexual orientation	7
	10	Recognising when a relationship is unhealthy or abusive (including the unacceptability of both emotional and physical abuse and violence including 'honour' based violence, forced marriage and rape) and strategies to manage this or access support for self or others at risk. Knowing about the impact of domestic abuse (including sources of help and support).	3
Self-Harm	10	Recognising and managing the triggers (for themselves or their friends) for unhealthy coping strategies, such as self-harm. Recognising when they or others need help, sources of help and strategies for accessing it.	1
Suicide	10	Recognising and managing the triggers (for themselves or their friends) for unhealthy coping strategies, such as self-harm. Recognising when they or others need help, sources of help and strategies for accessing it.	1
Anti-Semitism	10	To know about the unacceptability of all forms of discrimination and how to challenge it; prejudice and bigotry in the wider community including the workplace	1
Radicalisation and Extremism	KS1	Recognise and understand the meaning and differences between 'fact' and 'opinion'. Learn that beliefs are kinds of opinions that should be accepted, but not necessarily adopted. Recognise and know how to deal with situations involving peer pressure. Recognise and respect similarities and differences between people. Recognise and know how to deal with situations involving confrontation. Recognise that difference is a positive feature.	3
	KS2	Understand the meaning and importance of resilience and courage. Recognise and know how to deal with situations involving peer pressure. Recognise the features of extremism. Identify why and how people are recruited into extremist activities. Identify some of the stereotypes relevant to extremism. Understand how extremism can lead to harm. Recognise individuality and celebrate differences. Identify and challenge stereotypes, including LGBT and other minority groups. Recognise extremism and radicalisation. Identify the risks faced in relation to extremist activity. Understand how they can lead to harm.	5

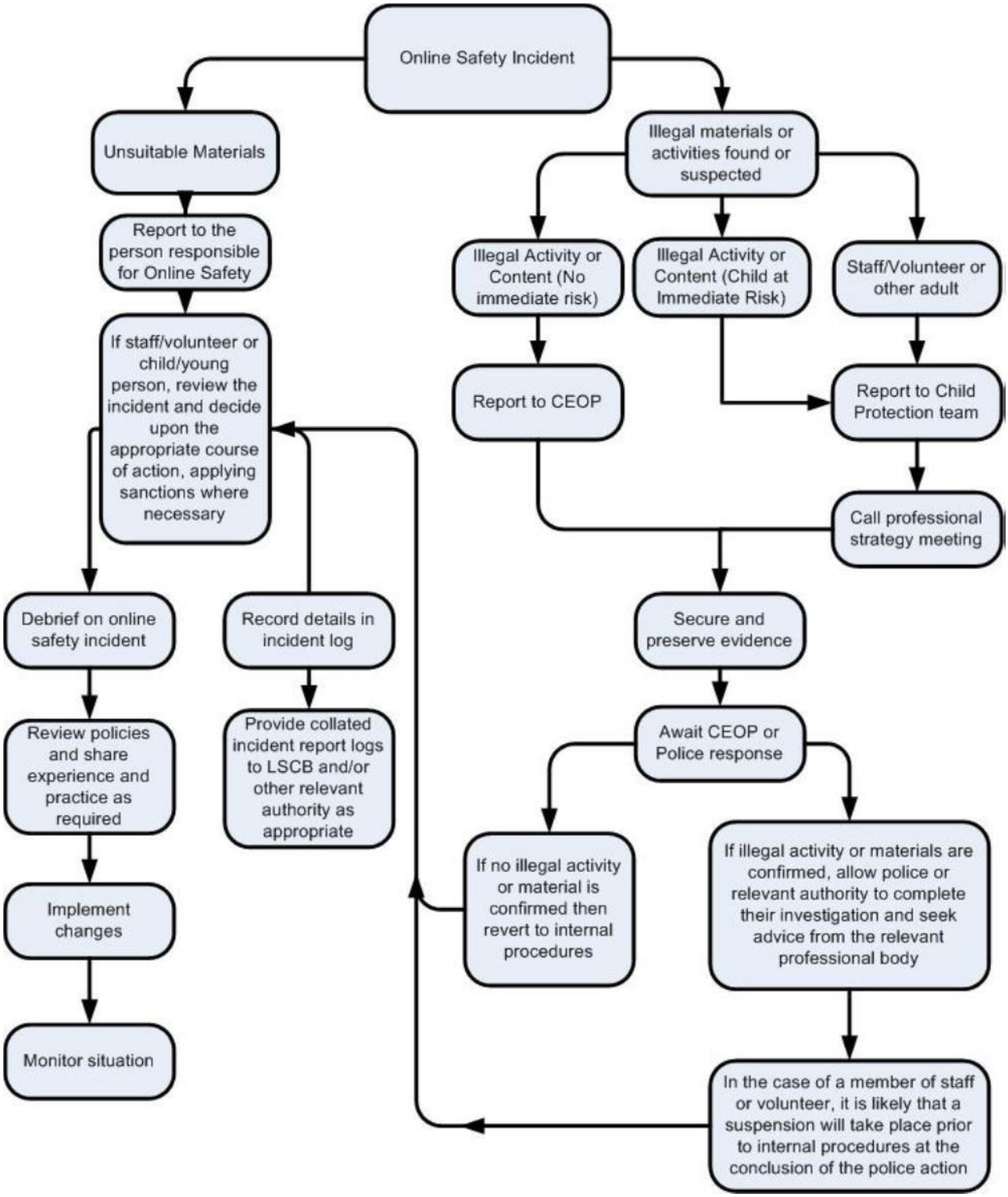
	8	Recognising the features of extremism. Identifying why and how people are recruited into extremist activities. Knowing why some people are vulnerable to radicalisation.	3
	9	Identifying why people are recruited into extremist activities. Knowing why some people are vulnerable to radicalisation. Understanding the consequences of radicalisation.	3
	10	Thinking critically about extremism and intolerance in whatever forms they take (including religious, racist and political extremism, the concept of 'shame' and 'honour based' violence). Recognising the shared responsibility to protect the community from violent extremism and how to respond to anything that causes anxiety or concern.	2
Peer to Peer Pressure	8	Recognising peer pressure. Developing strategies to manage peer pressure. Being aware of and understanding the feelings and pressure that the need for peer approval can generate.	2
	11	Managing peer pressure in relation to illicit substances. Assessing the risks of drug and alcohol abuse and addiction To develop strategies to manage peer and other influence around alcohol, tobacco and drug use.	1
Grooming or Exploitation for Sexual, Criminal, Financial or other Purposes	8	Recognising the risks associated with internet use. Understanding how online activities can expose you and others to risks.	2
	9	Awareness of exploitation and trafficking. Knowing what trafficking is and in particular child trafficking. Learning about the risks victims face.	1
	11	To develop an awareness of exploitation, bullying, harassment and control in relationships (including the unique challenges posed by online abuse and the unacceptability of physical, emotional, sexual abuse in all types of teenage relationships, including in group settings such as gangs) and the skills and strategies to respond appropriately or access support	1
Sexting	8	Understanding what the law says about E-Safety. Describing what is safe practice on the internet. Knowing where to get support. Recognising and describing potential dangers of the internet. Understanding how online activities can expose you and others to risks.	1¼
	9	It is illegal to send others anything that would be considered grossly offensive and cause distress or anxiety. Pupils should be made aware that once something is posted to the internet it is generally impossible to remove. Pupils should be aware that employers may search for them before they get a job. Pupils should	2

		think about things that could be posted online and how that may affect them in the future. Pupils should also think about how posting things about others could affect that person.	
Consent	9	Knowing that consent is freely given and that being pressurised, manipulated or coerced to agree to something is not 'consent'. Learning about the law in relation to consent.	1
	10	Knowing that living together, marriage and civil partnerships are ways that people freely and without coercion, demonstrate their commitment to each other. Understanding the role of sex in the media and its impact on sexuality – including sexual ethics such as consent, negotiation, boundaries, respect and right.	2
	11	Understanding the concept of consent in relevant, age-appropriate contexts building on KS3. Knowing how to seek consent and to respect others' right to give, not give or withdraw consent to engage in different degrees of sexual activity. Recognising when others are using manipulation, persuasion or coercion and how to respond.	2
Online Gambling	7 and 11	Why people gamble Different forms of gambling and their consequences The addictive nature of gambling To recognise and manage the influences on their financial decisions, (including managing risk, planning for expenditure, understanding debt and gambling in all its forms To know how to access appropriate support for financial decision-making and for concerns over money, gambling etc	3
Phishing	KS1	Learning about the importance of using the internet safely. Using strategies to stay safe when using ICT and the internet. Knowing that people sometimes behave differently online, including by pretending to be someone they are not.	1
	LKS2	Using ICT safely including keeping electronic data secure. Knowing how information and data is shared and used online.	1
	8	Recognising the risks associated with internet use. Understanding how online activities can expose you and others to risks.	1¼
	10	Knowing how information and data is generated, collected, shared and used online.	1
Trolling	KS1	Learning about the importance of using the internet safely. Using strategies to stay safe when using ICT and the internet. Knowing that the internet can also be a negative place where online abuse, trolling, bullying and harassment can take place, which can have a negative impact on mental health.	1

	LKS2	Know the rule and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them. Knowing where and how to report concerns and get support with issues online.	2
	UKS2	Knowing that the internet can also be a negative place where online abuse, trolling, bullying and harassment can take place, which can have a negative impact on mental health.	1
	8	Recognising and describing potential dangers of the internet. Understanding how online activities can expose you and others to risks.	1¼
Financial Scams	7 and 8	Recognising the risks associated with internet use. Understanding how online activities can expose you and others to risks. Pupils should look at what sort of information people put online, especially on social media. Pupils should be encouraged to identify what this data could be used for maliciously; some examples of this are identify theft or using location to identify when theft can take place.	2¼
Making or Sending Nudes	8	Understanding what the law says about E-Safety. Describing what is safe practice on the internet. Knowing where to get support. Recognising and describing potential dangers of the internet.	2
	9	It is illegal to send others anything that would be considered grossly offensive and cause distress or anxiety. Pupils should be made aware that once something is posted to the internet it is generally impossible to remove. Pupils should be aware that employers may search for them before they get a job. Pupils should think about things that could be posted online and how that may affect them in the future. Pupils should also think about how posting things about others could affect that person.	2
Online Bullying	KS1	Learning about the importance of using the internet safely. Using strategies to stay safe when using ICT and the internet. Knowing that the internet can also be a negative place where online abuse, trolling, bullying and harassment can take place, which can have a negative impact on mental health.	1
	LKS2	Know the rule and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them. Knowing where and how to report concerns and get support with issues online.	2
	UKS2	Know that bullying (including cyberbullying) has a negative and often lasting impact on mental wellbeing. Knowing how to critically consider their online friendships and sources of information including awareness of the risks associated with people they have	1

		never met. Knowing that the internet can also be a negative place where online abuse, trolling, bullying and harassment can take place, which can have a negative impact on mental health.	
	7	Types of bullying Recognising bullying and abuse in all its forms The impact of bullying Dealing with Online Bullying Pupils should look at different situations on both websites and social media and identify if it is bullying or not. Pupils should be encouraged to think about what effect the bullying could have to a person on both sides and why they might do it. Recognising and responding appropriately to online bullying.	1
	8	Knowing about online bullying and how to protect themselves.	1
Passwords	KS1	Learning about the importance of using the internet safely. Using strategies to stay safe when using ICT and the internet.	1
	LKS2	Know the rule and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them. Using ICT safely including keeping electronic data secure. Using ICT safely including using software features and settings.	2
	8	Knowing how to set privacy settings	2
Inappropriate or Illegal Websites	KS1	Learning about the importance of using the internet safely. Using strategies to stay safe when using ICT and the internet.	2
	LKS2	Know the rule and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them. Using ICT safely including keeping electronic data secure. Knowing why social media, some computer games and online gaming, for example, are age restricted.	2
	8	Recognising the risks associated with internet use. Understanding how online activities can expose you and others to risks.	¼

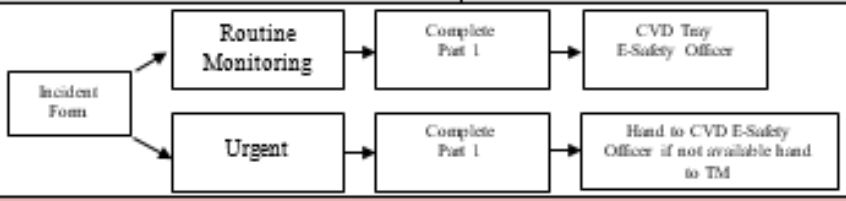
Appendix H: Flow chart for incidents



Appendix I: Incident investigation/reporting

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)