Marjory Kinnon School

Online Safety Policy

October 2025

This policy is based on a model ‘Online Safety Policy’ from The Key (reviewed 11 August 2025).

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors.
- Identify and support groups of pupils that are potentially at greater risk of harm online than others.
- 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, misinformation, disinformation (including fake news), conspiracy theories, racism, misogyny, self-harm, suicide, antisemitism, 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 the user 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 (RSE) and health 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.

3. 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 online safety at a level that they can understand including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of online safety issues.

For our pupils with difficulties in social understanding, careful consideration is given to group interactions when raising awareness of online 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.

4. Roles & Responsibilities

4.1 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 make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The Governing Body will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

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

The Governing Body will make sure that the school teaches pupils how to keep themselves and others safe, including online.

The Governing Body will make sure that the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The Governing Body will review the DfE filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting those standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems.
- Reviewing filtering and monitoring provisions at least annually.
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning.
- Having effective monitoring strategies in place that meet the school’s safeguarding needs.

The Governor who oversees online safety is: Paul Goulden.

All Governors will:

- Make sure 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 2).
- Make sure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is 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.

4.2 The Headteacher

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

4.3 The Designated Safeguarding Lead

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

The DSL (Amy Higgins) takes lead responsibility for online safety in school, in particular:

- Supporting the Headteacher in making sure that staff understand this Policy and that it is being implemented consistently throughout the school.
- Working with the Headteacher and Governing Body to review this policy annually and make sure the procedures and implementation are updated and reviewed regularly.
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks.
- Providing governors with assurance that filtering and monitoring systems are working effectively and reviewed regularly.
- Working with the ICT Manager to make sure the appropriate systems and processes are in place.
- Working with the Headteacher, ICT Manager 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's Safeguarding & Child Protection Policy.
- Responding to safeguarding concerns identified by filtering and monitoring.
- Making sure that any online safety incidents are logged (see Appendix 5) and dealt with appropriately in line with this Policy.
- Making sure 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 4 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.
- Undertaking annual risk assessments that consider and reflect the risks pupils face.
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively.

This list is not intended to be exhaustive.

4.4 The ICT Manager

The ICT Manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness and make sure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material.
- Making sure 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.

4.5 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.
- Reading (on EVERY) and agreeing / adhering to the terms of the Guidance for Acceptable Use of The Internet & Technologies (Appendix 3), and making sure that pupils follow the school's terms on acceptable use (Appendix 1).
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing by logging on either Every or MyConcern (as appropriate).
- Following the correct procedures by contacting the DSL if they need to bypass the filtering and monitoring systems for educational purposes.
- Working with the DSL to ensure that any online safety incidents are logged (see Appendix 5) 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.

4.6 Parents

Parents are expected to:

- Notify a member of staff or the Headteacher of any concerns or queries regarding this Policy.
- Make sure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (Appendix 1).

Parents/carers can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? – UK Safer Internet Centre.

- Help and advice for parents/carers – Childnet
- Parents and carers resource sheet – Childnet

4.7 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 of acceptable use (Appendix 2).

5. 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.
- Be discerning in evaluating digital content.

By the **end of primary school**, pupils will know:

- That the internet can be a negative place where online abuse, trolling, bullying and harassment can take place, which can have a negative impact on mental health.

- 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.
- How to be a discerning consumer of information online including understanding that information, including that from search engines, is ranked, selected and targeted.
- 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.
- The benefits of rationing time spent online, the risks of excessive time spent on electronic devices and the impact of positive and negative content online on their own and others' mental and physical wellbeing.
- Why social media, computer games and online gaming have age restrictions and how to manage common difficulties encountered online.
- How to consider the effect of their online actions on others and know how to recognise and display respectful behaviour online and the importance of keeping personal information private.
- Where and how to report concerns and get support with issues online.

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 that 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 similarities and differences between the online world and the physical world, including: the impact of unhealthy or obsessive comparison with others online (including through setting unrealistic expectations for body image), how people may curate a specific image of their life online, over-reliance on online relationships including social media, the risks related to online gambling including the accumulation of debt, how advertising and information is targeted at them and how to be a discerning consumer of information 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.

6. Educating Parents/Carers About Online Safety

The school will raise parents/carers' 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/carers.

Online safety will also be covered during parents' evenings.

The school will let parents/carers know:

- What systems the school uses to filter and monitor online use.
- What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online.

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.

7. Cyber Bullying

7.1 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's Behaviour Policy.)

7.2 Preventing & 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 encourage them 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 class.

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.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training. (See Section 12 for more detail).

The school also sends information / leaflets on cyber-bullying to parents/carers 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's 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 report the incident and provide the relevant material to the Police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

7.3 Examining Electronic Devices

The Headteacher and any member of staff authorised to do so by the Headteacher can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence.

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the Headteacher / DSL / appropriate staff member.
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it.
- Seek the pupil's co-operation.

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL, Headteacher or other member of the senior leadership team to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding whether there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the Police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent/carer refuses to delete the material themselves.

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image.
- Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people.

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.
- Our Behaviour Policy.

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

7.4 Artificial Intelligence (AI)

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Gemini.

Marjory Kinnon School recognises that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.

Marjory Kinnon School will treat any use of AI to bully pupils very seriously, in line with our Anti-bullying Policy.

Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by the school, and where existing AI tools are used in cases which may pose a risk to all individuals that may be affected by them, including, but not limited to, pupils and staff.

Any use of artificial intelligence should be carried out in accordance with our Artificial Intelligence (AI) Policy.

8. Acceptable Use of The Internet in School

All pupils, parents / carers, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (Appendices 1 - 3). 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 and restrict access through filtering systems where appropriate.

More information is set out in the acceptable use agreements in Appendices 1 to 3.

9. Pupils Using Mobile Devices in School

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

- Lessons.
- 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 (see Appendix 1).

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.

10. The Safe Use of Video Conferencing in School

To safely use video conferencing in school, staff must only use school-approved and secure video conferencing platforms.

Professional Standards

Staff must:

- Maintain professional conduct such as professional language, behaviour, and appropriate dress, as you would in a face-to-face setting.
- Be aware of their surroundings and conduct calls from a professional and appropriate area (e.g., office desk) or use a neutral or blurred background to protect privacy.
- Understand that calls can be recorded by anyone present.
- Avoid sharing personal information or using inappropriate chat functions.
- Report any concerns to the Designated Safeguarding Lead.

Technical Controls

- Set up meetings with password protection and lock them to prevent unwanted attendees.
- Utilise features like waiting rooms or "lobby" features to vet participants before they join.
- Keep software, apps, and devices updated to protect against vulnerabilities.
- Seek permission from everyone on the call before recording or using an AI meeting assistant.

Remote Learning Calls with Students

- Staff must only use apps or platforms agreed by the school to communicate with pupils, and it is the responsibility of the teachers to gatekeep and check content and comments.
- Have at least two staff members present in video calls with pupils or designate one staff member to supervise.
- Record sessions only with a legitimate, explicit purpose and ensure it doesn't replace other safeguarding measures.
- The call should be ended if a member of staff witnesses or hears anything of concern. Details will be passed to the DSL.

11. Staff Using Work Devices Outside School

All staff members will take appropriate steps to ensure their devices remain secure as set out in Home Working Section of the Guidance for Acceptable Use of Internet & Technologies. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords can be made up of 3 random words, in combination with numbers and special characters if required, or generated by a password manager.
- 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 by promptly installing 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 the Home Working Section of the Guidance for Acceptable Use of Internet & Technologies (Appendix 3).

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/ICT Manager.

12. 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 Behaviour Policy 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 Disciplinary Policy & Procedure. 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.

13. Training

13.1 Staff, Governors & Volunteers

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 3).

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, threatening, 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 Designated Safeguarding Lead and Deputy DSL 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.

13.2 Pupils

All pupils will receive age-appropriate training on safe internet use, including:

- Methods that hackers use to trick people into disclosing personal information.
- Password security.
- Social engineering.
- The risks of removable storage devices (e.g. USBs).
- Multi-factor authentication.
- How to report a cyber incident or attack.

- How to report a personal data breach.

Pupils will also receive age-appropriate training on safeguarding issues such as cyberbullying and the risks of online radicalisation.

14. Monitoring Arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in Appendix 5.

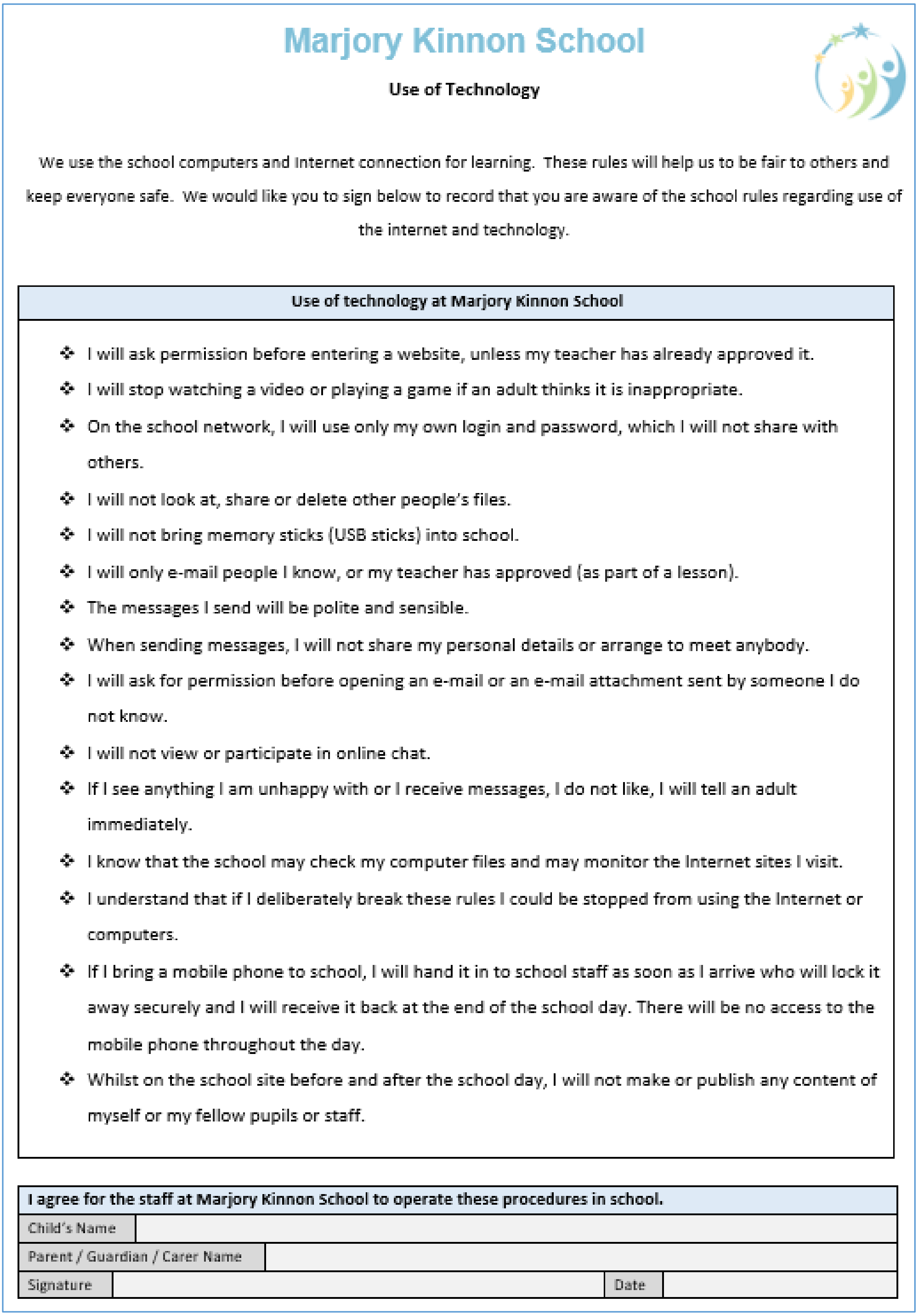
This policy will be reviewed every year by the Headteacher. At every review, the policy will be shared with the Governing Body. The review will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms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

15. 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.
- Artificial Intelligence (AI) Policy.
- Anti-bullying Policy.

Appendix 1: Pupil Acceptable Use Agreement (Pupils & Parents/Carers)



Marjory Kinnon School

Use of Technology

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 and technology.

Use of technology at Marjory Kinnon School

- I will ask permission before entering a website, unless my teacher has already approved it.
- I will stop watching a video or playing a game if an adult thinks it is inappropriate.
- On the school network, I will use only my own login and password, which I will not share with others.
- I will not look at, share or delete other people's files.
- I will not bring memory sticks (USB sticks) into school.
- I will only e-mail people I know, or my teacher has approved (as part of a lesson).
- The messages I send will be polite and sensible.
- When sending messages, I will not share my personal details or arrange to meet anybody.
- 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 view or participate in online chat.
- If I see anything I am unhappy with or I receive messages, I do not like, I will tell an adult 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.
- If I bring a mobile phone to school, I will hand it in to school staff as soon as I arrive who will lock it away securely and I will receive it back at the end of the school day. There will be no access to the mobile phone throughout the day.
- Whilst on the school site before and after the school day, I will not make or publish any content of myself or my fellow pupils or staff.

I agree for the staff at Marjory Kinnon School to operate these procedures in school.

Child's Name			
Parent / Guardian / Carer Name			
Signature		Date	

Appendix 2: Acceptable Use Agreement (Governors / Visitors)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET:
AGREEMENT FOR GOVERNORS AND VISITORS

Name of Governor / Visitor:

This Agreement forms part of the school's Online Safety Policy. It is designed to ensure that Governors, and Visitors are aware of their responsibilities when using any form of ICT. Governors and Visitors are expected to sign this agreement and adhere to its contents at all times.

Any concerns or clarification should be discussed with Amy Higgins, Online Safety Lead.

- 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) the Securus system will scan my laptop and if it detects inappropriate websites (including pornography, radicalisation, extremist views), Securus will save a screen shot that is then monitored by the Online Safety Team.
- 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 school's ICT system security by not disclosing any passwords provided to me by the school or other related authorities.
- I will ensure that all electronic communications are compatible with my professional role or visit to the school.
- 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 concern of professional conduct by the 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 or software without the permission of the ICT Team.
- I will not browse, download, upload or distribute any material to school networks or devices 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 to school networks or devices 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 the 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: (Governor/Visitor)	**Date:**

Appendix 3: Guidance for Acceptable Use of Internet & Technologies

This document has been developed to ensure staff at Marjory Kinnon School are aware of their professional responsibilities when using ICT equipment and systems. All staff will follow the guidelines at all times. You are responsible for your behaviour and actions when carrying out any activity which involves using ICT equipment and information systems, either within school or at other locations, such as home. ICT equipment and associated technologies include all facilities and resources used to access the school ICT network and internet as well as standalone devices with digital storage.

When using the school's ICT equipment and other information systems, I have understood and will comply with the following statements:

- I have read and understood the implications and my personal responsibilities in relation to the use of ICT equipment which is detailed within this guidance.
- I will access the internet and other ICT systems using an individual username and password, which I will keep secure. I will ensure that I log out after each session and never allow other users to access the internet through my username and password. I will report any suspicion, or evidence that there has been a breach of my personal security in relation to access to the internet or ICT systems.
- As a new starter, I will use the passwords created by the school to enable me to access the internet and ICT systems. I must change and create my own password.
- I will not share my passwords with any colleagues or pupils within school.
- I will not search for, download, upload or forward any content that is illegal or that could be considered offensive by another user. If I encounter any such material, I will report it immediately to the Online Safety Officer (Designated Safety Lead, Amy Higgins).
- I will take a professional and proactive approach to assessing the effectiveness of the internet content-filtering platform in relation to the educational content that can be viewed by the pupils in my care.
- I will not attempt to bypass any filtering and/or security systems put in place by the school. If I suspect a computer or system has been damaged or affected by a virus or other malware, I will report this to ICT staff.
- I will ensure that all devices taken off site (laptops, tablets, cameras, removable media or phones), will be secured in accordance with the school’s Data Protection Registration and any information-handling procedures both on and off site.

- I understand my personal responsibilities in relation to the Data Protection Act and the privacy and disclosure of personal and sensitive confidential information.
- I will secure any equipment taken off site for school trips.
- I will not store images or information about pupils or staff on any portable hard drive etc. and will only use school systems such as SharePoint, Tapestry and Arbor to record data or information about staff and pupils.
- I will not use USB sticks to store any type of school data and/or any information. I understand the use of the USB is not permitted in the school and will be actively blocked.
- I will ensure that any personal or sensitive information taken off site will be situated on a school-owned device with appropriate technical controls such as encryption / password / VPN protection deployed.
- Any information asset, which I create from other information systems, which could be deemed as personal or sensitive will be stored on the school network and access controlled in a suitable manner in accordance with the school data protection controls. (For example, spreadsheets/other documents created from information located within the school information management system).
- I will not download or install any software from the internet or from any other media which may compromise the school network or information situated on it without prior authorisation from ICT staff.
- I will return any school-owned ICT equipment or software to the relevant individual within school (ICT staff) once it is no longer required.
- I understand that the use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to the appropriate authorities.
- I understand that my files, communications and internet activity may be monitored and checked at all times to protect my own and others' safety, and action may be taken if deemed necessary to safeguard me or others.
- I understand that if I do not follow all statements in this Acceptable Use Guidance (AUG) and in other school policies relating to the use of ICT equipment, I may be subject to disciplinary action in line with the school's established disciplinary procedures.

Internet Usage

This guidance applies to all employees who have access to computers and the Internet to be used in the performance of their work. Use of the Internet by employees is permitted and encouraged where such use supports the goals and objectives of the school.

When using the school's internet, I have understood and will comply with the following statements:

- I understand I am expected to use the Internet responsibly and productively. Internet access is limited to job-related activities only and personal use is not permitted. Job-related activities include research and educational tasks that may be found via the Internet that would help me in my role.
- I understand that all Internet data that is composed, transmitted and/or received by the school's computer systems is considered to belong to Marjory Kinnon School and is recognized as part of its official data. It is therefore subject to disclosure for legal reasons or to other appropriate third parties.
- I understand that the equipment, services and technology used to access the Internet are the property of the school and that Marjory Kinnon School reserves the right to monitor Internet traffic and access data that is composed, sent or received through its online connections.
- I understand that all sites and downloads may be monitored and/or blocked by the school if they are deemed to be harmful and/or not productive to business.
- I will not install software such as instant messaging technology as this is strictly prohibited.
- If I am unsure about what constitutes acceptable Internet usage, then I will ask my line manager for further guidance and clarification.
- I understand it is my responsibility to report, to a member of the Senior Leadership Team, any concerns I may have regarding internet usage by staff or pupils in the school.

Social Media

- I must not talk about my professional role in any capacity when using personal social media such as Instagram, Facebook, X (formerly known as Twitter), LinkedIn and YouTube or any other online publishing websites.
- I must not use social media tools to communicate with current or former pupils under the age of 18.

- I will not use any social media tools to communicate with parents unless approved in writing by the Headteacher.
- I will set and maintain my profile on social networking sites to maximum privacy and give access to known friends only.
- I will not access social networking sites for personal use during school hours.
- If I experience any derogatory or slanderous comments relating to the school, colleagues or my professional status that I wish to report, I will take screenshots for evidence and report it to the Headteacher.

Managing Digital Content

- I will demonstrate professional, safe and responsible behaviour when creating, using and storing digital images, video and sound within school.
- I will only use school equipment to create digital images, video and sound. Digital images, video and sound will not be taken without the permission of participants. Images and video will be of appropriate activities and participants will be in appropriate dress. No resources will be published online without the permission of the staff and parents of the pupils involved.
- Under no circumstances will I use any personally-owned equipment for video, sound or images.
- When searching for images, video or sound clips, I will ensure that I or any pupils in my care are not in breach of any copyright law.
- I will ensure that any images, videos or sound clips of pupils are stored on the school network and never transferred to personally-owned equipment.
- I will ensure that any images taken on school-owned devices are transferred to the school network (storage area/server) and immediately deleted from the memory card.
- I will model safe and responsible behaviour in the creation and publishing of online content within the school learning platform and any other websites. In addition to this I will encourage colleagues and pupils to adopt similar safe behaviour in their personal use of blogs, wikis and online publishing sites.

Learning & Teaching

- I will support and promote the school Online Safety Policy at all times. I will model safe and responsible behaviour to pupils when using ICT to support learning and teaching.

- I will ensure that I am aware of my individual responsibilities relating to the safeguarding of children within the context of Online Safety and know what to do in the event of misuse of technology by any member of the school community.
- I understand the importance of respecting and acknowledging copyright of materials found on the internet and will model best practice in the creation of my own resources at all times.

Email

- I will use my school email address for all correspondence with staff, parents or other agencies and I understand that any use of the school email system will be monitored and checked. I will under no circumstances use my private email account for any school-related business.
- Communication between staff and pupils or members of the wider school community should be professional and related to school matters only.
- I will ensure that any posts made on websites or via electronic communication, by either myself or the pupils in my care, will not damage the reputation of my school.
- I will not synchronise any school email account with a personally-owned handheld device that is not password protected.
- I will take care in opening any attachments sent by email. I will only open emails and associated attachments from trusted senders. If unsure, I will check with ICT staff.
- Emails sent to external organisations will be written carefully and authorised before sending to protect myself. As and when I feel it necessary, I will carbon copy (cc) the Headteacher, my line manager or another suitable member of staff into the email.
- I will ensure that I manage my email account, delete unwanted emails and file those I need to keep in subject folders.
- I will access my school email account on a regular basis to ensure that I respond in a timely manner to communications that require my attention.

Mobile Phones & Devices

- I will ensure that my mobile phone and any other personally-owned device is switched off or switched to ‘silent’ mode during school hours.
- My mobile phone/device will be stored away in a safe location and not on my person unless in a prior arranged circumstance; or if I am on a clearly designated break; or if required for work use.

- I will not use my mobile phone/device during working hours except in exceptional circumstances such as an emergency or for a prior arranged circumstance or if I am on a clearly designated break or if required for work use.
- Bluetooth communication will be ‘hidden’ or switched off and mobile phones or devices will not be used during teaching periods unless permission has been granted by a member of the Senior Leadership Team in emergency circumstances.
- I will not connect any mobile device to the school’s wireless network at any time.
- I will not connect any mobile device to the school network at any time.
- I will not contact any parents or pupils on my personally-owned device.
- I will not use any personally-owned mobile device to take images, video or sound recordings.

Due to the nature of their work, some support staff (Site Team, Head of Operations, Operations Manager, Head of HR, Executive PA) and members of the Senior Leadership Team have special dispensation to use mobile phones in and around the school to assist with the smooth running of the school.

Home Working

Scope & Definitions

This applies to all staff who work from home and/or use or access school systems or information from home or while working remotely. This includes individuals who are given access to the school networks and data (including governors, students, visitors, volunteers, contractors and third parties). It applies to information in all formats, including paper records and electronic data.

Remote working means working off the school site. This includes working while connected to the school’s networks.

A mobile device is defined as a portable device which can be used to store or process information. Examples include but are not limited to laptops, tablets, USB sticks, removable disc drives and smartphones.

Remote or home working from a location outside of the UK, is not permitted as this would involve significant legal and practical issues, affecting both you and the school.

Homeworking may be requested by staff working in certain departments or roles with the exception of teachers, teaching assistants, caretakers, medical, attendance, front office, etc., as these roles can only be undertaken in the workplace. This does not form part of any contract of employment and the school may amend it at any time.

Awareness of Risk

Working from home presents both significant risks and benefits. Staff may have remote access to information held on secure school servers but without the physical protections available in school. Without the network protection provided by firewalls and access controls, there are much greater risks of unauthorised access to data as well as a risk of loss or destruction of data. There are also greater risks posed by information "in transit" (i.e., moving data between home and school).

The risks posed by working from home can be summarised under three headings:

- Reputational: The loss of trust or damage to the school's relationship with its community.
- Personal: Unauthorised loss of or access to data could expose staff or students to identity theft, fraud or significant distress.
- Monetary: Regulators such as the ICO can impose financial penalties and those damaged as a consequence of a data breach may seek redress through the courts.

Roles & Responsibilities

The decision as to whether to allow partial or full-time homeworking in relation to any given role rests with the Senior Leadership Team. Any member of staff working from home is responsible for ensuring that they work securely and protect both information and school-owned equipment from loss, damage or unauthorised access.

Line Managers are responsible for supporting staff adherence with this policy. Additional measures may be put in place by the SLT to ensure these rules are adhered to (for example, monitoring or supervision). Failure to comply with this guidance may result in disciplinary action.

Key Principles of Homeworking

Staff working from home must ensure that they work in a secure and authorised manner. This can be done by complying with the principles below: -

i. To adhere to the principles of the Data Protection Act 2018 and the school's Data Protection Policy in the same way as they would if they were working in school.

ii. Access to personal data must be controlled. This can be done through physical controls, such as locking the home office for physical data and locking the computer by using strong passwords (a mixture of letters, numbers and special characters).

iii. No other members of the household should know or be able to guess your password(s). If passwords are written down (which should be a last case scenario) they must be stored securely (e.g. in a locked drawer or in a secure password protected database). Passwords should never be left on display for others to see.

iv. Automatic locks should be installed on IT equipment used to process school information that will activate after a period of inactivity (i.e. computers should automatically lock requiring you to sign back in after a period of time).

v. IT equipment used to process and store school information in the home must be kept in a secure place where it cannot be easily accessed or stolen.

vi. Portable mobile devices used to process and store school information should be encrypted where possible (or at least password / pin code protected) and should never be left unattended in a public place.

vii. IT equipment in the home used to process school information should not be used where it can be overseen by unauthorised persons.

viii. It is the responsibility of each member of staff to ensure that they are working in a safe environment at home. No health and safety risks must be taken when using school equipment.

ix. Access to certain systems and services by those working from home or remotely may be deliberately restricted or may require additional authentication methods (such as two factor authentication which requires an additional device to verify individuals). Any attempt to bypass these restrictions may lead to disciplinary action.

x. All personal information and in particular sensitive personal information should be encrypted/password protected before being sent by email where possible. Extra care must be taken when sending emails where auto-complete features are enabled (as this can lead to sending emails to similar/incorrect email addresses). The rules relating to the sending of emails are outlined in this guidance.

xi. Staff should always use school email addresses when contacting colleagues or students. If telephoning a child or parent at their home, staff should ensure that their caller ID is blocked.

xii. Any technical problems (including but not limited to, hardware failures and software errors) which may occur on the systems must be reported to the ICT Manager immediately.

xiii. Staff must adhere to the school's Data Retention Policy and ensure that information held remotely is managed according to the data retention schedule. Data should be securely deleted and destroyed once it is no longer needed.

xiv. If communicating remotely via video conferencing and social media, staff must adhere to using only those platforms which have been approved by the school and follow guidance on the safe use of video conferencing in the Online Safety Policy.

xv. Staff should be vigilant to phishing emails and unsafe links. If clicked these links could lead to malware infection, loss of data or identity theft.

xvi. Staff should not access inappropriate websites on school devices or whilst accessing school networks.

xvii. Staff provided with school-owned IT equipment to work from home must:

a. Only use the equipment for legitimate work purposes.

b. Only install software on the equipment if authorised by the school's ICT Team. This includes screen savers, photos, video clips, games, music files and opening any documents or communications from unknown origins.

c. Ensure that the equipment is well cared for and secure.

d. Not allow non-staff members (including family, flatmates and friends) to use the equipment or to share log-in passwords or access credentials with them.

e. Not attempt to plug in memory sticks into the equipment unless encrypted and supplied by the school).

f. Not collect or distribute illegal material via the internet.

g. Ensure anti-virus software is regularly updated.

h. Return the equipment securely at the end of the remote working arrangement.

xviii. Staff are not allowed to use their own equipment to process school data.

xix. Staff are responsible for ensuring the security of school property and all information, files, documents, data, etc., within their possession, including both paper and electronic material. In particular, physical data (i.e. paper documents, which includes documents printed at home) must be secured and staff must ensure that:

a. Paper documents are not removed from the school without the prior permission of your Line Manager. When such permission is given, reasonable steps must be taken to ensure the confidentiality of the information is maintained during transit.

In particular, the information is not to be transported in see-through bags or other un-secured storage containers.

b. Paper documents should not be used in public places and not left unattended in any place where it is at risk (e.g. car boots, luggage rack on public transport).
c. Paper documents taken home or printed at home containing personal information, sensitive data and confidential information are not left around where they can be seen, accessed or removed.
d. Paper documents are collected from printers as soon as they are produced and not left where they can be casually read.
e. The master copy of the data is not to be removed from school premises.
f. Paper documents containing personal data are locked away in suitable facilities such as secure filing cabinets in the home just as they would be in school.
g. Documents containing confidential personal information are not pinned to noticeboards where other members of the household may be able to view them.
h. Paper documents are disposed of securely by shredding and should not be disposed of with the ordinary waste unless it has been shredded first.

xx. Any staff member provided with school devices must not do, cause or permit any act or omission which will avoid coverage under the school’s insurance policy. If in any doubt as to whether particular acts or omissions will have this effect, the staff member should consult their Line Manager immediately.

All staff must report any loss or suspected loss, or any unauthorised disclosure or suspected unauthorised disclosure, of any school-owned IT equipment or data immediately to the Chief Operating Officer ~~Headteacher~~ and the ICT Manager in order that appropriate steps may be taken quickly to protect school data. Failure to do so immediately may seriously compromise school security. Any breach which is either known or suspected to involve personal data or sensitive personal data shall be reported to the Data Protection Officer (whose details can be found in the Data Protection Policy).

Appendix 4: 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 Guidance for Acceptable Use of Internet & Technologies for staff / volunteers?	
Are you familiar with the school's acceptable use agreement for governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents/carers?	
Are you familiar with the filtering and monitoring systems on the school's devices and networks?	
Do you understand your role and responsibilities in relation to filtering and monitoring?	
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 5: 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**