



Online safety Policy

Scheme of Delegation	
Approval by:	FGB – to review in line with ethos
Staff Lead Reviewer:	Karen Corrigan
Assigned Governor:	Vanessa O'Reilly
Date of Last Approval:	1/7/26
Date of next review:	1/7/27
Review Cycle:	Annually
Publish:	Website

This Online policy should be read in conjunction with the Children's Acceptable Use Agreement (appendix 1), Device Loan Agreement – issued to all teachers who have a school laptop (appendix 2), the Staff Code of Conduct and all other safeguarding policies referenced below.

Contents

1. Aims
2. Legislation and guidance
3. Roles and responsibilities
4. Educating pupils about online safety
5. Cyber bullying
6. Acceptable use of the Internet in school
7. Pupils using mobile devices in school
8. Staff using work devices outside school
9. Training for staff, governors and volunteers
10. Monitoring

Appendix 1 – Acceptable use agreement for children

Appendix 2 – Device loan agreement for staff



Crowmarsh Gifford C of E Primary School

1. Aims

Crowmarsh Gifford Primary 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; and
- > **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

2. Legislation and guidance

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

- > [Teaching online safety](#)
- > [Meeting digital and technology standards](#)
- > [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. Roles and responsibilities

3.1 The governing board

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing board 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 board 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 board will co-ordinate regular meetings with appropriate staff to discuss online safety and requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

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

The governing board 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 board will review the [DfE's filtering and monitoring standards](#), and discuss with IT service providers what needs to be done to support the school in meeting the 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

All governors will:

- › Make sure they have read and understand this policy
- › Make sure that online safety is a running and interrelated theme when devising and implementing the whole-school approach to safeguarding and related policies and/or procedures
- › 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

3.2 The headteacher

The headteacher is responsible for making sure that staff understand this policy, and that it is being implemented consistently throughout the school.

3.3 The designated safeguarding lead (DSL)

Details of the school's designated safeguarding leads (DSL) are set out in our child protection and safeguarding policy, as well as relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

- › Making sure that staff understand this policy and that it is being implemented consistently throughout the school
- › Working with the governing board to review this policy and make sure the procedures and implementation are updated and reviewed regularly



Crowmarsh Gifford C of E Primary School

- › 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 Computing lead and IT support to make sure the appropriate systems and processes are in place
- › Working with staff and IT support, as necessary, to address any online safety issues or incidents
- › Managing all online safety issues and incidents in line with the school's child protection policy
- › Responding to safeguarding concerns identified by filtering and monitoring
- › Making sure that any online safety incidents are logged on CPOMS 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 as needed
- › Liaising with other agencies and/or external services if necessary
- › Providing regular reports on online safety in school to the governing board
- › 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.

3.4 The Computing lead and IT support

The Computing lead in conjunction with IT support are 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 IT 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 IT 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.

3.5 All staff and volunteers

All staff and volunteers are responsible for:

- › Maintaining an understanding of this policy
- › Implementing this policy consistently
- › Supporting the implementation of the Children's Acceptable Use agreement (appendix 1)
- › Following Acceptable Use requirements as set out in the Staff Code of Conduct and Device Loan Agreement (see section 8 and appendix 2)



Crowmarsh Gifford C of E Primary School

- › 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
- › Working with the DSL to make sure that any online safety incidents are logged on CPOMS and dealt with appropriately in line with this policy
- › Making sure 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.

3.6 Parents and carers

Parents and carers are expected to support the school by ensuring that their child understands and agrees to follow the Children's Acceptable Use Agreement.

Parents should raise any concerns that they have about in school Internet use and trust that this will be investigated effectively.

Parents are reminded at school events that they must not publish any photos containing children other than their own on social media. Parents are not permitted to post photos of staff on social media.

4. Educating pupils about online safety

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

All schools have to teach:

- › [Relationships education and health education](#) in primary schools

In **Key Stage (KS) 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 (KS) 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 people should be respectful in online interactions, and that the same principles apply to online relationships as to face-to-face relationships, including where people are anonymous. For example, the importance of avoiding putting pressure on others to share information and images online, and strategies for resisting peer pressure
- › How to critically evaluate their online relationships and sources of information, including awareness of the risks associated with people they have never met. For example, that people sometimes behave differently online, including pretending to be someone else, or pretending to be a child, and that this can lead to dangerous situations. How to recognise harmful content or harmful contact, and how to report this



Crowmarsh Gifford C of E Primary School

- › That there is a minimum age for joining social media sites (currently 13), which protects children from inappropriate content or unsafe contact with older social media users, who may be strangers, including other children and adults
- › The importance of exercising caution about sharing any information about themselves online. Understanding the importance of privacy and location settings to protect information online
- › Online risks, including that any material provided online might be circulated, and that once a picture or words has been circulated there is no way of deleting it everywhere and no control over where it ends up
- › That the internet contains a lot of content that can be inappropriate and upsetting for children, and where to go for advice and support when they feel worried or concerned about something they have seen or engaged with online
- › How to report a range of concerns

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.

4.2 Pupils will be taught practical cyber security skills

Pupils in KS2 will receive age-appropriate training on safe internet use when appropriate, 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 education on safeguarding issues such as cyberbullying and the risks of online radicalisation.

5. Cyber-bullying

5.1 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 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

5.2 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 encourage them to do so, including where they are a witness rather than the victim.

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.



Crowmarsh Gifford C of E Primary School

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy.

The DSL will work with external services including the police, if it is deemed necessary to do so.

5.3 Artificial intelligence (AI)

Generative 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.

Crowmarsh Gifford Primary School recognises that AI has many uses to help pupils learn, but may also carry risks and have the potential to be used to bully others.

Crowmarsh Gifford Primary School will treat any use of AI to bully pupils very seriously, in line with the behaviour policy.

6. Acceptable use of the internet in school

All staff are expected to follow the Acceptable Use Agreement as set out in the Staff Code of Conduct and Device Loan Agreement (see section 8 and appendix 2)

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.

7. Pupils using mobile devices in school

No pupil at Crowmarsh Gifford Primary School requires a mobile device for the purpose of learning. Children in Year 5 and 6 are permitted to have mobile devices when they are walking to and from school unaccompanied. In this case all mobile devices are switched off and stored in the office during the school day.

In exceptional circumstances, a mobile device acting as medical equipment will be permitted in class.

8. Staff using work devices outside school

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

- › Keeping the device password-protected
- › 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

All members of staff who have been loaned a school laptop and have permission to take this device off site, will have signed and agree to adhere to a Device Loan Agreement (appendix 2)

If staff have any concerns over the security of their device, they must seek advice from the Computing lead who will report to IT support.



Crowmarsh Gifford C of E Primary School

9. Training for staff, governors and 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 staff members will receive refresher training at least once each academic year as part of safeguarding

10. Monitoring

Internet use at Crowmarsh Gifford Primary School is monitored through Smoothwall. Smoothwall is a technology system which constantly monitors all school digital devices for risky behaviours including but not limited to, bullying, self-harm, grooming and radicalisation. Concerns are generated through a combination of AI and human monitoring and alerts are quickly sent to the Headteacher for further investigation. Smoothwall meets all of the digital monitoring requirements and legislation set out in KCSIE 2025.



Appendix 1

Acceptable Use Agreement for Children

This agreement will be shared annually with all children during an Acceptable Use Agreement assembly, will be shared with parents and will be referred to by school staff as needed throughout the year.

All aspects of Acceptable Use for staff, governors and parents are covered in the Crowmarsh Gifford School Online Safety Policy.

Digital technologies have become an integral part of life, both within schools and outside school. These are powerful tools, which provide new opportunities for everyone. These technologies can stimulate discussion, promote creativity and create awareness of context to promote effective learning.

As a primary school, we recognise that children need clear teaching, consistent routines and trusted adults to help them navigate the online world. We therefore take a whole-school approach to online safety that links safeguarding, behaviour, curriculum, pastoral support and secure use of school systems. Online safety is taught in an age appropriate manner through our Computing and PSHE curriculum.

At Crowmarsh Gifford Primary School, we want all members of our school community to use digital technology safely, responsibly and with confidence. We believe that children should be entitled to safe internet access at all times. This Acceptable Use Agreement is intended to ensure that:

- our pupils will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
- school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- parents and guardians are aware of the importance of e-safety and are involved in the education and guidance of young people regarding on-line behaviour.

As a **pupil** of Crowmarsh Gifford School, I agree to the following -

When I use computers, tablets, the internet or other digital devices, I will keep myself and others safe

- I will be kind and respectful
- I will use kind words and be polite online.
- I will not send or share messages that are unkind, or hurtful.
- I will treat other people online the same way I want to be treated.
- I will always use my own username and password when logging onto a school device.
- I will not share my full name, address, phone number, school name, or photos on any website or social media.
- I will tell a teacher or trusted adult if something online makes me feel worried, upset, or uncomfortable.

I will use the internet responsibly

- I will only visit websites and use apps that my teacher has asked me to.
- I will not interfere with the school filters or safety settings.
- I will only use the internet for learning and school activities unless my teacher says otherwise.

I will look after school equipment

- I will handle computers and tablets carefully.
- I will not change settings or download anything without permission.
- I will report any damage or problems to an adult straight away.



Crowmarsh Gifford C of E Primary School

I will use photos and videos properly

- I will not take photos or videos of others unless a teacher says it is allowed.
- I will not share photos, videos, or work that does not belong to me without permission.

If something goes wrong

- I understand that if I do not follow these rules there may be consequences to my use of the Internet and devices at school
- I understand that the school uses 'Smoothwall' to monitor Internet use. I know that this means that any search on the Internet that is not appropriate to my age or my lesson, will be quickly and automatically reported to the headteacher.

If I am in Year 5 or 6 and I bring my own mobile phone to school

- My phone must be switched off and stored in the office for the school day
- I will not use my phone at all on the school site including taking photos
- I understand that my own mobile phone will never be required in the classroom.

Exceptions on an individual basis will be made to this where a mobile phone is required as a medical device.

I know that these rules help keep everyone safe.



Appendix 2

Device Loan Agreement for Staff

1. This agreement is between:

1) Crowmarsh Gifford CE Primary School ("the school")

2) ("the employee" and "I")

It governs the use and care of devices assigned to individual staff members. This agreement covers the period from the date the device is issued through to the return date of the device to the school.

All issued equipment shall remain the sole property of the school and is governed by the school's policies.

1. The school is lending the employee a laptop ("the equipment") for the purpose of working at school and at home.

2. This agreement sets the conditions for the employee taking the equipment home.

I confirm that I have read the terms and conditions set out in the agreement and my signature at the end of this agreement confirms that I have read and agree to these terms.

2. Damage/loss

By signing this agreement I agree to take full responsibility for the equipment issued to me and I have read or heard this agreement read aloud and understand the conditions of the agreement.

I understand that I am responsible for the equipment at all times whether on the school's property or not.

If the equipment is damaged, lost or stolen, I will immediately inform Vania Eaglen and/ or Karen Corrigan, and I acknowledge that I am responsible for full replacement costs. If the equipment is stolen, I will also immediately inform the police.

I agree to keep the equipment in good condition and to return it to the school on demand from the school in the same condition.

I will not leave the equipment unsupervised in unsecured areas.

3. Unacceptable use

I am aware that the school can monitor my activity on the equipment.

I will not carry out any activity that constitutes 'unacceptable use'.

This includes, but is not limited to:

- Accessing, creating, storing or linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate
- Sharing confidential information about the school, its pupils, or other members of the school community
- Setting up any software, applications or web services on this device without approval by authorised personnel, or creating or using any programme, tool or item of software designed to interfere with the functioning of the ICT facilities, accounts or data
- Carrying out any activity which defames or disparages the school, or risks bringing the school into disrepute
- Using inappropriate or offensive language

I accept that if I engage in any activity that constitutes 'unacceptable use', I may face disciplinary action in line with the school's policies on staff discipline/staff code of conduct.



Crowmarsh Gifford C of E Primary School

4. Personal use

I will not use this device for any personal use and will not loan the equipment to any other person.

5. Data protection

I agree to take the following measures to keep the data on the device protected.

- Keep the equipment 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)
- Make sure the equipment locks if left inactive for a period of time
- Do not share the equipment among family or friends
- Update antivirus and anti-spyware software as required
- Install the latest updates to operating systems, as prompted

If I need help doing any of the above, I will contact Karen Corrigan on the email ktwo1968@crowmarsh-gifford.oxon.sch.uk

6. Return date

I will return the device in its original condition to Karen Corrigan within 14 days of being requested to do so.

I will return the equipment to the school upon resignation, dismissal or if I leave the employment of the school for any other reason.

7. Consent

By signing this form, I confirm that I have read and agree to the rules and conditions above.

FULL NAME

SIGNATURE