Great Waltham C of E Primary School

Online Safety Policy

	Name of School	**Great Waltham Primary School**
	Policy review Date	**November 2026**
	Date of next Review	**November 2027**
	Who reviewed this policy?	**SLT / Governors**

This policy is part of the School's Statutory Safeguarding Policy. Any issues and concerns with online safety must follow the school's safeguarding and child protection processes.

Contents

1. Introduction and Overview

- Rationale and Scope
- Roles and responsibilities
- How the policy is communicated to staff/pupils/community
- Handling complaints
- Reviewing and Monitoring

2. Education and Curriculum

- Pupil online safety curriculum
- Staff and governor training
- Parent awareness and training

3. Expected Conduct and Incident Management

4. Managing the IT Infrastructure

- Internet access, security (virus protection) and filtering
- Network management (user access, backup, curriculum and admin)
- Passwords policy
- E-mail
- School website
- Learning platform
- Social networking
- Video Conferencing

5. Data Security

- Management Information System access
- Data transfer
- Asset Disposal

6. Equipment and Digital Content

- Personal mobile phones and devices
- Digital images and video

1. Introduction and Overview

Rationale

The purpose of this policy is to:

- Set out the key principles expected of all members of the school community at Great Waltham Primary School with respect to the use of IT-based technologies.
- Safeguard and protect the children and staff.
- Assist school staff working with children to work safely and responsibly with the Internet and other IT and communication technologies and to monitor their own standards and practice.
- Set clear expectations of behaviour and/or codes of practice relevant to responsible use of the Internet for educational, personal or recreational use for the whole school community.
- Have clear structures to deal with online abuse such as online bullying.
- Ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- Minimise the risk of misplaced or malicious allegations made against adults who work with pupils.

The main areas of risk for our school community can be summarised as follows:

Content

- Exposure to inappropriate content
- Lifestyle websites promoting harmful behaviours
- Hate content
- Content validation: how to check authenticity and accuracy of online content

Contact

- Grooming (sexual exploitation, radicalisation etc.)
- Online bullying in all forms
- Social or commercial identity theft, including passwords

Conduct

- Aggressive behaviours (bullying)
- Privacy issues, including disclosure of personal information
- Digital footprint and online reputation
- Health and well-being (amount of time spent online, gambling, body image)
- Sharing nudes or semi-nudes
- Copyright (little care or consideration for intellectual property and ownership)

Scope

This policy applies to all members of Great Waltham Primary School community (including staff, pupils/pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of school IT systems, both in and out of Great Waltham Primary School.

Roles and responsibilities

Role	Key Responsibilities
• Headteacher	• Must be adequately trained in offline and online safeguarding, in-line with statutory guidance and relevant Safeguarding partners • To lead a 'safeguarding' culture, ensuring that online safety is fully integrated with whole school safeguarding • To take overall responsibility for online safety provision • To take overall responsibility for data management and information security (SIRO) ensuring school's provision follows best practice in information handling • To ensure the school uses appropriate IT systems and services including, filtered Internet Service • To be responsible for ensuring that all staff receive suitable training to carry out their safeguarding and online safety roles • To be aware of procedures to be followed in the event of a serious online safety incident • Ensure suitable 'risk assessments' undertaken so the curriculum meets needs of pupils, including risk of children being radicalised • To ensure that there is a system in place to monitor and support staff who carry out internal online safety procedures, e.g. network manager • To ensure Governors are regularly updated on the nature and effectiveness of the school's arrangements for online safety • To ensure school website includes relevant information • The Designated Safeguarding Lead (DSL) has day-to-day responsibility for overseeing online safety
Designated Child Protection Lead and Computing Curriculum Leader	• Take day to day responsibility for online safety issues and a leading role in establishing and reviewing the school's online safety policy/documents • Promote an awareness and commitment to online safety throughout the school community • Ensure that online safety education is embedded within the curriculum • Ensure the school follows the latest DfE guidance (Filtering and monitoring)

Role	Key Responsibilities
	• Liaise with school technical staff where appropriate • To communicate regularly with SLT to discuss current issues. • To ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident • Ensure the school completes an annual online safety risk review (as part of safeguarding procedures) which reflects the current risks faced by pupils. • To ensure that online safety incidents are logged as a safeguarding incident • Facilitate training and advice for all staff • Oversee any pupil surveys / pupil feedback on online safety issues • Liaise with the Local Authority and relevant agencies • Is regularly updated in online safety issues and legislation, and be aware of the potential for serious child protection concerns.
Governors/Safeguarding governor (including online safety)	• To ensure that the school has in place policies and practices to keep the children and staff safe online • To approve the Online Safety Policy and review the effectiveness of the policy • To support the school in encouraging parents and the wider community to become engaged in online safety activities • To be aware of anonymised online safety incidents. • Review filtering and monitoring arrangements at least annually and following any safeguarding incident involving online activity. • Ensure filtering and monitoring systems are effective.
Computing Curriculum Leader	• To oversee the delivery of the online safety element of the Computing curriculum
Network Manager/technician (LaserTech)	• To report online safety related issues that come to their attention, to the Online Safety Coordinator • To manage the school's computer systems, ensuring - systems are in place for misuse detection and malicious attack (e.g. keeping virus protection up to date) - access controls/encryption exist to protect personal and sensitive information held on school-owned devices - the school's policy on web filtering is applied and updated on a regular basis • That they keep up to date with the school's online safety policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant

Role	Key Responsibilities
	• That the use of school technology and online platforms are regularly monitored and that any misuse/attempted misuse is reported to the online safety co-ordinator/Headteacher • To ensure appropriate backup procedures and disaster recovery plans are in place • To keep up-to-date documentation of the school's online security and technical procedures
Data and Information (Asset Owners) Managers (IAOs)	• To ensure that the data they manage is accurate and up-to-date • Ensure best practice in information management. i.e. have appropriate access controls in place, that data is used, transferred and deleted in-line with data protection requirements. • The school must be registered with Information Commissioner
Teachers	• To embed online safety in the curriculum • To supervise and guide pupils carefully when engaged in learning activities involving online technology • To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws • Ensure vulnerable children, children who have experienced abuse and pupils with SEND receive adapted online safety teaching if deemed necessary.
All staff, supply teachers and governors.	• To read, understand, sign and adhere to the school Code of conduct (8. Acceptable use of technology) • To report any suspected misuse or problem to the DSL • To maintain an awareness of current online safety issues and guidance through CPD • To model safe, responsible and professional behaviours in their own use of technology • Staff must not upload personal, confidential or safeguarding information into generative AI tools unless explicitly approved and compliant with the school's data protection policies. Staff should critically evaluate AI-generated content before using it for educational purposes • Receive training on the school's filtering and monitoring systems and understand how to report concerns regarding their effectiveness **Exit strategy** • At the end of the period of employment to return any equipment or devices loaned by the school. This will include leaving PIN numbers,

Role	Key Responsibilities
	IDs and passwords to allow devices to be reset, or meeting with line manager and technician on the last day to log in and allow a factory reset.
Pupils	• To understand the importance of reporting abuse, misuse or access to inappropriate materials • To know what action to take if they or someone they know feels worried or vulnerable when using online technology • To understand the importance of adopting safe behaviours and good online safety practice when using digital technologies out of school and realise that the school's online safety policy covers their actions out of school • To contribute to any 'pupil voice' / surveys that gathers information of their online experiences
Parents/carers	• To consult with the school if they have any concerns about their children's use of technology • To support the school in promoting online safety

Communication:

The policy will be communicated in the following ways:

- Policy to be posted on the school website.
- Policy to be part of school induction pack for new staff.
- Regular updates and training on online safety for all staff.
- Acceptable use agreements discussed with staff and pupils at the start of each year.

Handling Incidents:

- The school will take all reasonable precautions to ensure online safety.
- Staff and pupils are given information about infringements in use and possible sanctions.
- Computing Curriculum Leader/DSL acts as first point of contact for any incident.
- Any suspected online risk or infringement is reported to Computing Curriculum Leader/DSL that day
- Any concern about staff misuse is always referred directly to the Headteacher, unless the concern is about the Headteacher in which case the compliant is referred to the Chair of Governors.

Review and Monitoring

The online safety policy is referenced within other school policies

- The online safety policy will be reviewed every year or when any significant changes occur with regard to the technologies in use within the school
- There is widespread ownership of the policy and it has been agreed by the SLT and approved by Governors.

2. Education and Curriculum

Pupil online safety curriculum

Great Waltham Primary School:

- has a clear, progressive online safety education programme as part of the computing curriculum. This covers a range of skills and behaviours appropriate to their age and experience;
- plans online use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas;
- ensures staff are aware of their responsibility to model safe and responsible behaviour in their own use of technology, e.g. use of passwords, logging-off, use of content, research skills, copyright;
- ensures that staff and pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright;

- ensure pupils only use school-approved systems and publish within appropriately secure / age-appropriate environments.
- Will educate pupils about Cyber-bullying bullying that takes place through digital technologies, including social media, messaging platforms, online gaming and other internet-enabled services. Through our progressive online safety curriculum, pupils are taught how to recognise, prevent and respond to cyber-bullying, understand its impact on others, and know how to report concerns.

Staff and governor training

This school:

- makes regular training available to staff on online safety issues and the school's online safety education program;
- provides, as part of the induction process, all new staff with information and guidance on the Online Safety Policy.

Parent awareness and training

Great Waltham Primary School:

- provides induction for parents which includes online safety;
- runs a rolling programme of online safety advice, guidance and training for parents.

3. Expected Conduct and Incident management

Expected conduct

At Great Waltham Primary School, all users:

- are responsible for using the school IT and communication systems in accordance with the Code of Conduct;
- understand the significance of misuse or access to inappropriate materials and are aware of the consequences;
- understand it is essential to reporting abuse, misuse or access to inappropriate materials and know how to do so;
- understand the importance of adopting good online safety practice when using digital technologies in and out of school;
- know and understand school policies on the use of mobile and hand held devices including cameras, smart watches & smart glasses;

Staff, volunteers and contractors

- know to be vigilant in the supervision of children at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas where older pupils have more flexible access;
- know to take professional, reasonable precautions when working with pupils, previewing websites before use; using age-appropriate (pupil friendly) search engines where more open Internet searching is required with younger pupils;

Parents/Carers

- should know and understand what the school's 'rules of appropriate use for the whole school community' are and what sanctions result from misuse.

Incident Management

At Great Waltham Primary School:

- there is strict monitoring and application of the online safety policy and a differentiated and appropriate range of sanctions;
- all members of the school are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the school's escalation processes;
- support is actively sought from other agencies as needed (i.e. the local authority, UK Safer Internet Centre helpline, CEOP, Prevent Officer, Police) in dealing with online safety issues;
- monitoring and reporting of online safety incidents takes place and contribute to developments in policy and practice in online safety within the school;
- parents/carers are specifically informed of online safety incidents involving young people for whom they are responsible;
- the Police will be contacted if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law;
- we will immediately refer any suspected illegal material to the appropriate authorities – Police, Internet Watch Foundation and inform the LA.

4. Managing IT and Communication System

Internet access, security (virus protection) and filtering

Great Waltham Primary School:

- has the educational filtered secure broadband connectivity;
- uses an Education filter which blocks sites that fall into unauthorised categories. All changes to the filtering policy are logged and only available to staff with the approved 'web filtering management' status;
- ensures network health through use of anti-virus software;

- Uses DfE, LA or ECC approved systems including DfE S2S, to send 'protect-level' (sensitive pupil) data over the Internet
- Uses encrypted devices or secure remote access where staff need to access 'protect-level' (sensitive personal) data off-site;
- Works in partnership with the ECC to ensure any concerns about the system are communicated so that systems remain robust and protect pupils.

Network management (user access, backup)

Great Waltham Primary School

- Uses individual, audited log-ins for all users
- Uses guest accounts occasionally for external or short-term visitors for temporary access to appropriate services;
- Has daily back-up of school data (admin and curriculum);
- Uses secure, 'Cloud' storage for data back-up that conforms to DfE guidance;
- All processing of personal data will comply with UK GDPR and the Data Protection Act 2018

To ensure the network is used safely, this school:

- Ensures staff read and understand the school's online safety Policy. All pupils have their own unique username and password which gives them access to the Internet and other services;
- Makes clear that no one should log on as another user and makes clear that pupils should never be allowed to log-on or use teacher and staff logins;
- Has set-up the network with a shared work area for pupils and one for staff. Staff and pupils are shown how to save work and access work from these areas;
- Requires all users to log off when they have finished working or are leaving the computer unattended;
- Ensures all equipment owned by the school and/or connected to the network has up to date virus protection;
- Makes clear that staff are responsible for ensuring that any computer or laptop loaned to them by the school, is used primarily to support their professional responsibilities.
- Maintains equipment to ensure Health and Safety is followed;
- Ensures that access to the school's network resources from remote locations by staff is audited and restricted and access is only through school/LA approved systems;
- Does not allow any outside Agencies to access our network remotely except where there is a clear professional need and then access is audited restricted and is only through approved systems;
- Has a clear disaster recovery system in place that includes a secure, remote off site back up of data;

- This school uses secure data transfer; this includes DfE secure S2S website for all CTF files sent to other schools;
- Ensures that all pupil level data or personal data sent over the Internet is password protected.
- Our wireless network has been secured to appropriate standards suitable for educational use;
- All IT and communications systems installed professionally and regularly reviewed to ensure they meet health and safety standards;

Password policy

- This school makes it clear that staff and pupils must always keep their passwords private, must not share with others; If a password is compromised the school should be notified immediately and the password should be changed.
- All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password(s) private.
- We require staff to use STRONG passwords and to uses MFA where available

E-mail

Great Waltham Primary School

- Provides staff with an email account for their professional use, and makes clear personal email should be through a separate account;
- Will contact the Police if one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law.
- Will ensure that email accounts are maintained and up to date
- Will use a number of EEC provided technologies to help protect users and systems in the school, including desktop anti-virus product McAfee/Panda, plus direct email filtering for viruses.

Pupils:

- Online safety education is delivered through the Computing curriculum and through the school's PSHE curriculum. This includes online relationships, media literacy, misinformation, online bullying, online scams, digital footprints, privacy, online reputation, artificial intelligence, and seeking support from trusted adults

Staff:

- Staff will use Office 365 e-mail systems for professional purposes
- Access in school to external personal e mail accounts may be blocked
- Never use email to transfer staff or pupil personal data. 'Protect-level' data should never be transferred by email. If there is no secure file transfer solution available for the situation, then the data / file must be protected with security encryption.

School website

- The Headteacher, supported by the Governing body, takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained;
- The school web site complies with statutory DFE requirements;
- Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status;
- Photographs published on the web do not have full names attached. We do not use pupils' names when saving images in the file names or in the tags when publishing to the school website;

Social networking

Staff, Volunteers and Contractors

- Staff are instructed to always keep professional and private communication separate.
- Teachers are instructed not to run social network spaces for student use on a personal basis or to open up their own spaces to their pupils, but to use the schools' preferred system for such communications.

School staff will ensure that in private use:

- No reference should be made in social media to pupils, parents/carers or school staff;
- School staff should not be online friends with any pupil. Any exceptions must be approved by the Headteacher.
- They do not engage in online discussion on personal matters relating to members of the school community;
- Personal opinions should not be attributed to the school or local authority and personal opinions must not compromise the professional role of the staff member, nor bring the school into disrepute;
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Pupils:

- Are taught about social networking, acceptable behaviours and how to report misuse, intimidation or abuse through our online safety curriculum work.
- Pupils will be taught to critically evaluate online content, including content generated by artificial intelligence tools, and understand that images, videos and written content may be manipulated or misleading.
- Pupils are required to sign and follow our [age appropriate] pupil Acceptable Use Agreement.

Parents:

- Are reminded that they need to ask permission before uploading photographs, videos or any other information about other people.

5. Data security: Management Information System access and Data transfer

Strategic and operational practices

At Great Waltham Primary School:

- The Head Teacher is the Senior Information Risk Officer (SIRO).
- Staff are clear who are the key contact(s) for key school information (the Information Asset Owners) are. We have listed the information and information asset owners.
- We ensure staff know who to report any incidents where data protection may have been compromised.
- All staff are DBS checked and records are held in a single central record

Technical Solutions

- Staff have secure area(s) on the network to store sensitive files.
- Details of all school-owned hardware will be recorded in a hardware inventory.
- Details of all school-owned software will be recorded in a software inventory.
- Disposal of any equipment will conform to the appropriate legislation which can be found on the Environment Agency website.

6. Equipment and Digital Content

Mobile Devices (Mobile phones, tablets and other SMART devices including air tags, watches, & glasses)

- Mobile and SMART devices brought into school are entirely at the staff member, pupils & parents or visitors own risk. The School accepts no responsibility for the loss, theft or damage of any phone or hand held device brought into school.
- Mobile and SMART devices brought in to school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally-owned mobile devices.
- Pupils should not bring mobile phones or SMART devices to school unless agreed in advance by the Headteacher. Any phones brought onto site will be handed in to the office immediately and stored securely.
- Personal devices should not be used in areas where pupils are present unless there is a clear professional purpose (e.g. to log on to platforms as part of 2 step authentication)
- All visitors are requested to keep their phones on silent.

- The recording, taking and sharing of images, video and audio on any personal mobile device is to be avoided, except where it has been explicitly agreed by the Headteacher. Such authorised use is to be recorded. All mobile device use is to be open to monitoring scrutiny and the Headteacher is able to withdraw or restrict authorisation for use at any time, if it is deemed necessary.
- In line with DfE searching, screening and confiscation guidance the school reserves the right to search the content of any mobile devices on the school premises where there is a reasonable suspicion that it may contain illegal or undesirable material, including pornography, violence or bullying.

Staff use of personal devices

- Staff will be issued with a school phone where contact with pupils, parents or carers is required, for instance for off-site activities.
- In an emergency where a staff member doesn't have access to a school-owned device, they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes and then report the incident with the Headteacher / Designated Officer.
- If a member of staff breaches the school policy then disciplinary action may be taken.

Digital images and video

In this school:

- We gain parental/carer permission for use of digital photographs or video involving their child when their daughter/son joins the school.;
- We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials/DVDs;
- The school blocks/filter access to social networking sites unless there is a specific approved educational purpose;
- Pupils are taught about how images can be manipulated in their online safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children as part of their computing scheme of work;
- Pupils are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.
- Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.