CREETING ST MARY CofE PRIMARY SCHOOL

Online Safety and Acceptable Use Policy

Date of Policy	October 2026
Review Date	October 2027
Head Teacher's signature	Mrs C Friar
Chair of Governors' signature	Mrs M Brame

Aims.

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors.
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones' but is not restricted to these)
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

The 4 key categories of risk: Our approach to online safety is based on addressing the following categories of risk:

Content – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.

Contact – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.

Conduct – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and seminudes and/or pornography), sharing other explicit images and online bullying; and

Commerce – risks such as online gambling, inappropriate advertising, phishing and/or financial scam.

AI Purpose and Scope

This clause defines the permitted, responsible, and safe use of Artificial Intelligence (AI) and Generative AI tools (e.g., large language models, image generators, and automated content creators) by all students, staff, and visitors. This policy applies to all school-owned devices, personal devices connected to the school network, and any use of AI for school-related work or assessment.

1. General Principles

The school recognises AI as a valuable tool for learning and administrative efficiency. However, its deployment must align with the school's core commitment to data privacy, safeguarding, and academic integrity. AI must enhance, not replace, human critical thinking, teaching, and learning.

2. Permitted and Approved Use

Staff Use: Staff may use AI tools to assist with lesson planning, resource creation, and administrative tasks, provided they use school-approved or enterprise-grade systems vetted for data privacy.
Student Use: Students may only use AI tools when explicitly directed by a teacher for specific educational activities.
Authorised Tools: Only AI platforms officially approved by the school's IT and Data Protection officers may be accessed on school networks.

3. Data Protection and Privacy (Strict Restrictions)

No Personal Data: Users must **never** input personal, identifiable, or confidential data into public or unvetted AI tools. This includes student names, grades, behavior reports, staff details, or medical records.
No School IP: Uploading proprietary school materials, curriculum plans, or student work to public models for training purposes is strictly prohibited.
Age Restrictions: Users must comply with the minimum age terms of service specified by individual AI platform providers.

4. Academic Integrity and Coursework

Plagiarism and Misrepresentation: Submitting AI-generated content as a student's own original work constitutes academic malpractice.
Transparency: If AI is used as a research aid (where permitted by the teacher), students must explicitly cite the tool used, the prompt given, and the specific output generated.

5. Safeguarding and Content Safety

Inappropriate Content: Using AI tools to generate, search for, or manipulate harmful, illegal, defamatory, or inappropriate material is a severe breach of school discipline.
Critical Evaluation: Users must critically evaluate AI outputs. AI systems can produce "hallucinations" (factually incorrect information) or biased perspectives. AI content should never be accepted as an absolute source of truth.
Reporting: Staff and students must immediately report any safety risks, inappropriate content generation, or data exposure caused by AI tools to the Designated Safeguarding Lead (DSL) or IT department.

6. Enforcement and Misuse
Non-compliance with this policy will be treated under the school's standard disciplinary procedures. Sanctions may include loss of network privileges, disciplinary action for staff, or academic penalties and suspension for students.

Legislation and 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 cyberbullying:
- Advice for headteachers and school staff 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. Staff are also aware of the content of and amendments made to 'Keeping Children Safe in Education'

Roles and responsibilities

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

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

All governors will:

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

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

The designated safeguarding leads: will take lead responsibility for online safety in school, in particular:

- Support the whole community in ensuring that staff understand this policy and that it is being implemented consistently throughout the school.
- Work with the headteacher, ICT support provider and other staff, as necessary, to address any online safety issues or incidents.
- Manage all online safety issues and incidents in line with the school child protection policy, ensuring that any online safety incidents are logged with a DSL and dealt with appropriately in line with this policy.
- Ensure that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy.
- Update and deliver staff training on online safety.
- Liaise with other agencies and/or external services if necessary.
- Provide reports on online safety in school to the headteacher and/or governing body.

The Online Safety Lead with our ICT support provider

provider is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material.
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly conducting a full security check and monitoring the school's ICT systems on a regular basis.
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.
- Ensuring that any online safety incidents are recorded for Safeguarding File, logged with a DSL and dealt with appropriately in line with this policy.
- Ensuring that any incidents of online-bullying are dealt with appropriately in line with the school Positive Behaviour Policy and recorded in Safeguarding Files

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

- Maintaining an understanding of this policy and implementing it consistently
- Agreeing and adhering to the terms in the staff code of conduct and ensuring that pupils follow the school's terms on acceptable use.
- Working with the DSL to ensure that any online safety incidents are logged 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 Positive 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'.

Parents are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy.
- Notify the school of any online issues they are aware of that involves their child or other children at the school

Parents can seek further guidance on keeping children safe online from the following organisations and websites: What are the issues? – UK Safer Internet Centre Hot topics – Childnet International Parent resource sheet – Childnet International Healthy relationships – Disrespect Nobody

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

Educating pupils about online safety:

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

In Key Stage 1, pupils will be taught to:

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

Pupils in Key Stage 2 will be taught to:

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

By the end of primary school, pupils will know:

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

Educating parents about online safety:

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website. If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with a DSL.

Bullying

Definition

Online bullying takes place online, such as through social networking sites, messaging apps or gaming sites. It is the same as, and be treated, as all other forms of bullying, which are repetitive, intentionally seeking to harm one person or group by another person or group, where the relationship involves an imbalance of power.

Preventing and addressing bullying that takes place online.

To help prevent bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim. Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyberbullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate. In relation to a specific incident of online bullying, the school will follow the processes set out in the school Anti Bullying Policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained. The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

Examining electronic devices:

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

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to: Cause harm, and/or Disrupt teaching, and/or break any of the school rules.

If inappropriate material is found on the device, it is up to the Headteacher in conjunction with the DSL to decide whether they should: Delete that material, or Retain it as evidence (of a criminal offence or a breach of school discipline), and/or Report it to the police.

Staff may also confiscate devices for evidence to hand to the police, if a pupil discloses that they are being abused and that this abuse includes an online element. Any searching of pupils will be carried out in line with: The DfE's latest guidance on screening, searching and confiscation UKCIS guidance on sharing nudes and seminudes: advice for education settings working with children and young people and the school's.

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

Acceptable use of the internet in school:

All **pupils, parents, volunteers and governors** are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet.

School staff sign the Code of Conduct, which includes 'online expectations' in accordance with this policy, the law, KCSIE 'Teaching Standards', 'Professional Standards for Teaching Assistants' and their terms and conditions of employment.

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 the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above. More information is set out in the acceptable use agreements and the staff code of conduct.

Pupils using mobile devices in school:

If a pupil needs to bring a mobile device to school, the following applies.

- A parent/carer must give permission.
- The phone must be checked in/out of the office, not kept by the child during the school day.
- The school cannot take any responsibility for loss or damage.
- Any use of mobile devices in school by pupils must be in line with the acceptable use agreement.

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

Staff using work devices outside school: will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol).
- Making sure the device is locked if left inactive for a period of time.
- Not sharing the device among family or friends.
- Staff members will not use the device in any way which would violate the school's terms of acceptable use, as set out in the staff code of conduct.
- Work devices will be used solely for work activities. If staff have any concerns over the security of their device, they must seek advice from the school ICT provider or DSL.

How the school will respond to issues of misuse:

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

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

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

Training:

All new staff members will receive training, as part of their induction, on safe internet use and safeguarding issues including online-bullying and the risks of radicalisation. All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

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

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

Training will also help staff:

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

The DSL and deputies: 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 child protection and safeguarding policy.

Monitoring arrangements:

Individual pupil Safeguarding Files include concerns for behaviour and safeguarding issues related to online safety. The DSL should be informed of any incident they will monitor trends to look for individual pupils or issues affecting a group of pupils. This policy will be reviewed every two years. At every review, the policy will be shared with the Governing Body.

Links with other policies

This online safety policy is linked to our: Child Protection and Safeguarding Policy, Positive Behaviour Policy, Staff Disciplinary Procedures, Data Protection Policy, Complaints Procedure, ICT and Internet Acceptable Use statements and the staff Code of Conduct

Parent/Carers Acceptable Use Policy 2023

I have read and discussed the Acceptable Use Policy with my child

I know that my child will receive digital (online) safety education to help them understand the importance of safe use of technology and the internet, both in and out of school.

I am aware that any internet and computer use using school equipment is monitored for safety and security reasons and to safeguard both my child and the schools systems. This monitoring will take place in accordance with data protection and human rights legislation.

I understand that the school will take all reasonable precautions to ensure that pupils cannot access inappropriate materials but I appreciate that this is a difficult task. I understand that the school cannot be held responsible for the content of materials accessed through the Internet and the school is not liable for any damages arising from use of the Internet facilities

I understand that if the school has any concerns about my child's safety online, either at school or at home, then I will be contacted. I also understand that if my child does not abide by the school Acceptable Use Policy then sanctions will be applied in line with the schools behaviour and anti-bullying policy. If the school believes my committed a contacted

I, together with my child, will support the school's approach to digital safety and will not deliberately upload or add any images, video, sounds or text that could upset, threaten the safety of or offend any member of the school community

I know that I can speak to the school digital safety Coordinator, my child's teacher or the Head Teacher if I have any concerns about digital safety

I will visit the school website www.st-thomas-canterbury.kent.sch.uk/e-safety/ for more information about the school's approach to digital safety as well as to access useful links to support both myself and my child in keeping safe online at home

I will visit www.thinkuknow.co.uk/parents, www.nspcc.org.uk/onlinesafety www.internetmatters.org www.saferinternet.org.uk and www.childnet.com for more information about keeping my child(ren) safe online

I will support the school and my child by sharing responsibility and role modelling safe and positive online behaviour for my child and by discussing online safety with them when they access technology at home

School Governor Digital 'Acceptable Use' Policy

As an organisation with responsibility for children's safeguarding it is important that all staff and volunteers take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft. All, have a responsibility to use the school's computer system in a professional, lawful, and ethical manner. To ensure this some volunteers and all governors will read and sign this Acceptable Use Policy. This is not an exhaustive list and you are reminded that digital use on any platform should be consistent with the school ethos, other appropriate school policies, relevant national and local guidance and expectations, and the Law.

I understand that 'digital' includes networks, data and data storage, online and offline communication technologies and access devices. Examples include mobile phones, smart watches, PDAs, digital cameras, email and social media sites.

School owned information systems including TEAMS, must be used appropriately. I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.

I understand that any hardware and software provided by Creeting St Mary CofE Primary School can only be used by members of staff and governors and only for educational use. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or locking my login as appropriate.

I will respect system security and I will not disclose any password or security information. I will use a 'strong' password (A strong password has numbers, letters and symbols, with 8 or more characters, does not contain a dictionary word and is only used on one system).

I will not attempt to install any purchased or downloaded software, including browser toolbars, or hardware or to add anyone from outside of the school community to the school TEAMs account without permission from the system manager.

I will ensure that any school data or reports (that mention or contain information about or could identify pupils, staff or parents/carers) are kept in accordance with the Data Protection Act 1998. This means that all personal data will be obtained and processed fairly and lawfully, only kept for specific purposes, held no longer than necessary and will be kept private and secure with appropriate security measures in place, whether used in the workplace, hosted online (only within countries or sites with suitable data protection controls that meet the EU and UK regulations) or accessed remotely (e.g. via VPN). Any data which is being removed from the school site (such as via email or on memory sticks or CDs) will be encrypted by a method approved by the school.

I will not keep or access documents which contain school-related sensitive or personal information (including images, files, videos, emails etc.) on any personal devices (such as laptops, digital cameras, mobile phones), unless they are suitably secured and encrypted. I will use the School Platform within TEAMS to upload any work documents and files. I will protect any devices or passwords in my care from unapproved access or theft.

I will not store any personal information on the school system that is unrelated to school activities, such as personal photographs, files or financial information.

I will respect copyright and intellectual property rights.

I will report all incidents of concern regarding digital safety to the Designated Safeguarding Lead Lisa D'Agostini and/or the Online Safety Lead Carol Brooker as soon as possible. I will report any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable websites to Carol Brooker and or any other DSL in her absence.

I will not attempt to bypass any filtering and/or security systems put in place by the school.

My electronic communications with staff, parents/carers will take place within clear and explicit boundaries and will be transparent and open to scrutiny at all times. All communication will take place via school approved communication channelsTEAMS, phone call from school office and not via personal devices or communication channels e.g. social networking or mobile phones.

I will ensure that my online reputation and my use of digital and information systems are compatible with my role.

I will not create, transmit, display, publish or forward any material that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring my professional role, the school, or the County Council, into disrepute.

If I have any queries or questions regarding safe and professional practise online either in school or off site, then I will raise them with the Digital Safety Coordinator or the Head Teacher.

I understand that my use of the information systems, Internet and email on school systems may be monitored and recorded to ensure policy compliance. The School may exercise its right to monitor the use of information systems, including Internet access and the interception of e-mails in order to monitor compliance with this Acceptable Use Policy and the School's Data Security Policy. Where it believes unauthorised and/or inappropriate use of the service's information system or unacceptable or inappropriate behaviour may be taking place, the School will invoke its disciplinary procedure. If the School suspects that the system may be being used for criminal purposes or for storing unlawful text, imagery or sound, the matter will be brought to the attention of the relevant law enforcement organisation.

Staff Social Networking Acceptable Use Policy

As part of the school's drive to encourage safe and appropriate behaviour in the use of today's technology, I will support the school's approach to Digital Safety. I am aware that the social media (such as Facebook) is a public and global communication tool and that any content posted may reflect on the school, its reputation and services. I will not use social media to express any personal opinions or create, transmit, display, publish or forward any material that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring the school into disrepute.

I will not disclose information, make commitments or engage in activities on behalf of the school without authorisation from the school Digital Safety Coordinator Mrs Brooker and/or the head teacher. The head teacher retains the right to remove or approve content posted on behalf of the school.

I will ensure that any content posted abides by copyright and intellectual property rights, child protection legislation, privacy and data protection law and other relevant civil and criminal legislation.

I will follow the school's policy regarding confidentiality and data protection/use of images. This means I will ensure that the school has written permission from parents/carers before using images or videos which include any members of the school community. Any images of pupils will be taken on school equipment, by the school and in accordance with the school image policy. Images which include pupils will only be uploaded by the school. These will be for the sole purpose of inclusion and will not be forwarded to any other person or organisation.

I will promote digital safety in the use of social media and will help to develop a responsible attitude to safety online and to the content that is accessed or created. If publishing on behalf of the school, I will ensure that the communication has been appropriately risk assessed and approved by a member of senior leadership team/e-Safety coordinator/head teacher prior to use.

If administering social networking tools on behalf of the school, I will set up a specific account/profile using a school provided email address to administrate the account/site/page and I will use a strong password to secure the account. Personal social networking accounts or email addresses are not to be used. The school Digital Safety coordinator and/or school leadership team/head teacher will have full admin rights to any social networking sites I set up on behalf of the school.

Where it believes unauthorised and/or inappropriate use of social networking or unacceptable or inappropriate behaviour may be taking place on social networks, the school will exercise the right to ask for the content to be deleted or deactivated.

I will ensure that the content and channel is suitable for the audience and will be sensitive in the tone of language used and will ensure content is written in accessible plain English.

I will report any accidental access or receipt of inappropriate materials or inappropriate comments to the Digital Safety coordinator, head teacher and/or Designated Child Protection Coordinator urgently.

I will ensure that the social networking site/page is moderated on a regular basis as agreed with the school e-Safety coordinator.

I have read and understood the school Digital Safety policy which covers the requirements for safe ICT use, including using appropriate devices and the safe use of social media. I have ensured that the site has been suitably risk assessed and this use has been agreed by the head teacher.

If I have any queries or questions regarding safe and acceptable practise online I will raise them with the Digital Safety Coordinator, Designated Child Protection Coordinator or the head teacher.