



**Teversham Church of England
Primary School**

Online Safety Policy

2026-2028

DATE ADOPTED: 22 June 2026

REVIEW DATE: July 2028

Contents

- The background to this policy
- Rationale
- The online safety curriculum
- Continued Professional Development
- Mobile phones and Use of Mobile Data in School
- Monitoring, and adverting online safety incidents
- Responding to online safety incidents
- Appendices (including AUPs)

Background to this policy:

The purpose of this policy is to describe the safeguarding measures in place for adults and children in school in relation to online safety, including:

- The policies and practice embedded in our school and followed by the whole school community
- The infrastructure and how it is set up to keep pupils safe online, including monitoring, and preventing and responding to online safety incidents
- A progressive, relevant age-appropriate online safety curriculum for all pupils which (as a minimum) meets the requirements of the National Curriculum for Computing and the statutory Relationships and Health Education.

Online safety in schools is primarily a safeguarding and not a computing / technology one. Therefore this policy should be viewed alongside other Safeguarding policies and approaches including, but not limited to:

- Acceptable Use Policy (AUP)
- Safeguarding and Child Protection
- Personal Social and Health Education (PSHE)
- Safer Working Practices
- Data Protection / GDPR Policy
- Anti-Bullying Policy
- School Complaints Procedure
- [Cambridgeshire Progression in Computing Capability Materials](#)
- Whistle Blowing Procedure

This policy must be read alongside the staff and pupil Acceptable Use Policies attached as appendices. These AUPs outline the expectations and sanctions which apply to staff and pupil use of technology.

- The development of our safety policy involved:
 - The Headteacher
 - The Designated Safeguarding Lead
 - The Computing Subject Leader
 - Cambridgeshire Local Authority Advisor (Cambridgeshire Education ICT Service)

It was presented to the governing body on and ratified in June 2026 and will be formally reviewed in June 2028.

- This policy may also be partly reviewed and / or adapted in response to specific online safety incidents or developments in the school's use of technology. It has been shared with all staff via email and is readily available on the school network and website, and has also been made available to parents.
- All staff must be familiar with this policy and all staff and pupils must sign the relevant Acceptable Use Policy before being allowed to access school's systems (see appendices). As Online safety is an important part of strategic leadership within the school, all staff have a shared responsibility to ensure that the policy and practices are embedded. This will be monitored by the Headteacher, the Designated Safeguarding Lead and governors as appropriate.

Rationale:

- At Teversham CofE Primary School we believe that the use of technology in schools brings great benefits. To live, learn and work successfully in an increasingly complex and information-rich society, our children must be able to use technology effectively.

The use of these exciting and innovative technology tools in school and at home has been shown to support learning and promote pupil achievement. Yet at the same time, we recognise that the use of these new technologies can put young people at risk within and outside the school.

The risks they may face can broadly be categorised into the '4 C's' **Contact, Content, Conduct and Commerce** (Keeping Children Safe in Education) and may include:

- Access to harmful, illegal or otherwise unsuitable content including gaming, gambling sites, sexually explicit material and websites with extremist ideologies and images
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet, including the sharing of Self-Generated Indecent Images
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others
- Cyber-bullying
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading or streaming of music or video files
- Phishing or financial scams
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

While children and young people need support to keep them safe online, the risks associated with the use of technology are not restricted to just them. Online safety issues can also affect adults who work or are associated with the school and this will be referenced in more detail later in this policy.

Technologies regularly used by pupils and staff include:

Staff:

- Staff laptops, iPads, desktops, server access and access to MIS systems.
- Some staff have access to school systems beyond the school building (e.g. MIS systems, cloud storage e.g. Microsoft 365 of school files). Staff devices can also be used at home in accordance with the staff AUP, particularly with regard to GDPR.
- Staff level internet access
- Class cameras and other peripherals such as visualisers and Interactive Whiteboards
- School website

- School mobile phone
- School social media platforms

Pupils:

- Curriculum laptops / iPads including filtered access to the Internet and pupil level access to areas of the school network
- Cameras and peripherals including programming resources (Beebots, control equipment, class cameras etc.)
- Online learning platform (Microsoft Teams, Google Docs)

Where the school changes the use of existing technology or introduces new technologies which may pose risks to pupils' safety, a risk assessment will be completed to show how the risk is being mitigated and reduced to an acceptable level.

The online safety curriculum:

When using online technologies, it is essential that children understand how to behave in a safe and responsible manner and also how to react when faced with inappropriate content or situations which make them feel uncomfortable. The need for a progressive, age-appropriate online safety curriculum is clearly documented in the [National Curriculum for Computing \(England\)](#) and the statutory [Relationship and Health Education](#).

At Teversham CofE Primary School we believe that a comprehensive programme of online safety education is vital for developing our pupils' ability to use technologies safely. We believe that just as children learn how to swim by going to a swimming pool so they will learn safe life-long online behaviours by accessing and using a range of online services including the World Wide Web.

This is achieved using a combination of:

- Discrete and embedded activities drawn from a selection of appropriate materials and is linked to demonstrating safe practice in our online learning platform
- Our programme for online safety education is evidenced in teachers' planning both as discrete, embedded and continuous activities. Key safety messages are focused on during a specific e-safety week in school, these are then continuously revisited and discussed in every computing lesson.
- Key online safety messages are delivered and reinforced through cross curricular opportunities such as emailing, researching, blogging and communicating in appropriate online environments.

Continued Professional Development:

- Staff at Teversham CofE Primary School receive information and training on online safety issues in the form of staff meetings and updates from the school's online safety and Designated Safeguarding Leads, as well as training from external providers where appropriate.
- Nominated members of staff receive more in-depth training to support them in keeping up to date and reviewing the school's approach, policies and practice.
- New staff receive information on the school's acceptable use policy as part of their induction.
- All staff have been made aware of 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.

School website:

The main purpose of our school website is to provide information. Our school website will not only tell the world that our school exists, but it will provide information to our pupils and parents, promote the school to prospective ones and publish the statutory information required by the Department for Education.

Our school website can be used to showcase examples of pupils' work - in words, pictures, sound or movie clips - and can share resources for teaching and learning both within the school and with colleagues elsewhere.

Under safeguarding responsibilities, it is the duty of a school to ensure that every child in their care is safe, and the same principles should apply to the virtual presence of a school as it would apply to its physical surroundings. Head teachers and the Governing Body should therefore take on the responsibility to ensure that no individual child can be identified or contacted either via, or as a result of, information displayed on the school website.

Mobile phones and use of data in school:

Keeping Children Safe in Education acknowledges that "many children have unlimited and unrestricted access to the internet via mobile phone networks (i.e. 3G, 4G and 5G)." It highlights the need for schools to have a clear policy statement on, and carefully consider *"how this is managed on their premises and reflect this in their mobile and smart technology policy and their child protection policy."*

Children are not permitted to have a mobile phone in school. If by agreement with the Headteacher and parents that a child needs to have access to it whilst travelling to and from school, then they must hand the phone into the school office/Y6 teacher at the start of the day and collect it before leaving the site at the end of the day. Children who require access to their mobile phone for medical purposes (ie diabetics) will have access to their phone during the day, but their use of the mobile phone is carefully monitored.

Monitoring, and averting online safety incidents:

The school keeps children safe when using online technologies through a combination of online safety education, filtering and monitoring children's online activity and reporting incidents, including following Safeguarding procedures where appropriate.

The school's technology infrastructure is designed to minimise the risks associated with adult and pupil use of technology. Safeguards built into the school's infrastructure include:

- Secure, private JISC internet connection. This is provided and maintained by Everything ICT
- Managed firewalling running Unified threat management (UTM) that provides restrictions on download of software, apps and file types from known compromised sites.
- Enhanced web filtering provided via Netsweeper
- Antivirus package provided as part of the ICT services package
- Email system for all school staff with direct internal routes to the council for trusted email communications.

Staff also monitor pupils' use of technology and, specifically, their activity online. This is achieved through a combination of:

- Appropriate levels of supervision when pupils are using online technologies.
- Auto-generated alerts flag up activity in specific safeguarding categories which may raise child protection concerns.
- Staff are also able to monitor pupils' activity in the online environment (Microsoft Teams), allowing them to identify inappropriate or concerning online behaviour, as well as respond to reports of any such behaviour from pupils or parents.

Staff use of the schools' internet can also be monitored and investigated when needed.

A system of staff and pupil passwords is in place to enable appropriate access to the school network.

- All members of staff have individual, password protected logins to the school network / cloud service / MIS systems.

- All children have individual, password protected logins to the cloud services, e.g. Microsoft 365.
- Visitors to the school can access part of the school systems using a generic visitor login and password.
- The wireless network is encrypted to the standards advised by the Local Authority and the wireless key is kept securely by the school office.
- School staff and pupils are not permitted to connect personal devices to the schools' wireless network and the wireless password is only issued to visitors on a case-by-case basis.

Whilst we recognise that it is impossible to totally eliminate the risks associated with the use of technology, these safeguards are in place to help minimise these risks as much as possible.

Responding to online safety incidents:

It is important that all members of staff – teaching and non-teaching – are aware of how to respond if an online safety incident occurs or they suspect a child is at risk through their use of technology.

- Staff responses to online safety incidents must be consistent with responses to other incidents in school. This may mean that serious actions have to be taken in some circumstances.
- If an online safety incident occurs, Teversham CofE Primary School will follow its agreed procedures for responding including internal sanctions and involvement of parents (this may include the deactivation of accounts or restricted access to systems as per the school's AUPs or reporting incidents to the police or other authorities – see appendix).

In addition, the Education and Inspections Act 2006 empowers headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other online safety incidents which may take place outside of the school but has an impact within the school community.

- With this in mind, the headteacher may decide to apply the sanctions and / or procedures in the relevant AUP to incidents which occur outside of schools if s/he deems it appropriate.

The Education Act 2011 gives school staff the powers, in some circumstances, to search personal digital devices and decide whether or not to delete data or files if the person thinks there is good reason to do so.

However, there is a risk that this could conflict with guidance about dealing with incidents where a child may be at risk where it may be inadvisable to delete, save or share content. The school will always seek to resolve areas of concern in line with safeguarding procedures, and with parents where appropriate, before taking any further action.

This policy was ratified on: 22 June 2026

This policy will be reviewed: July 2028

Signed:

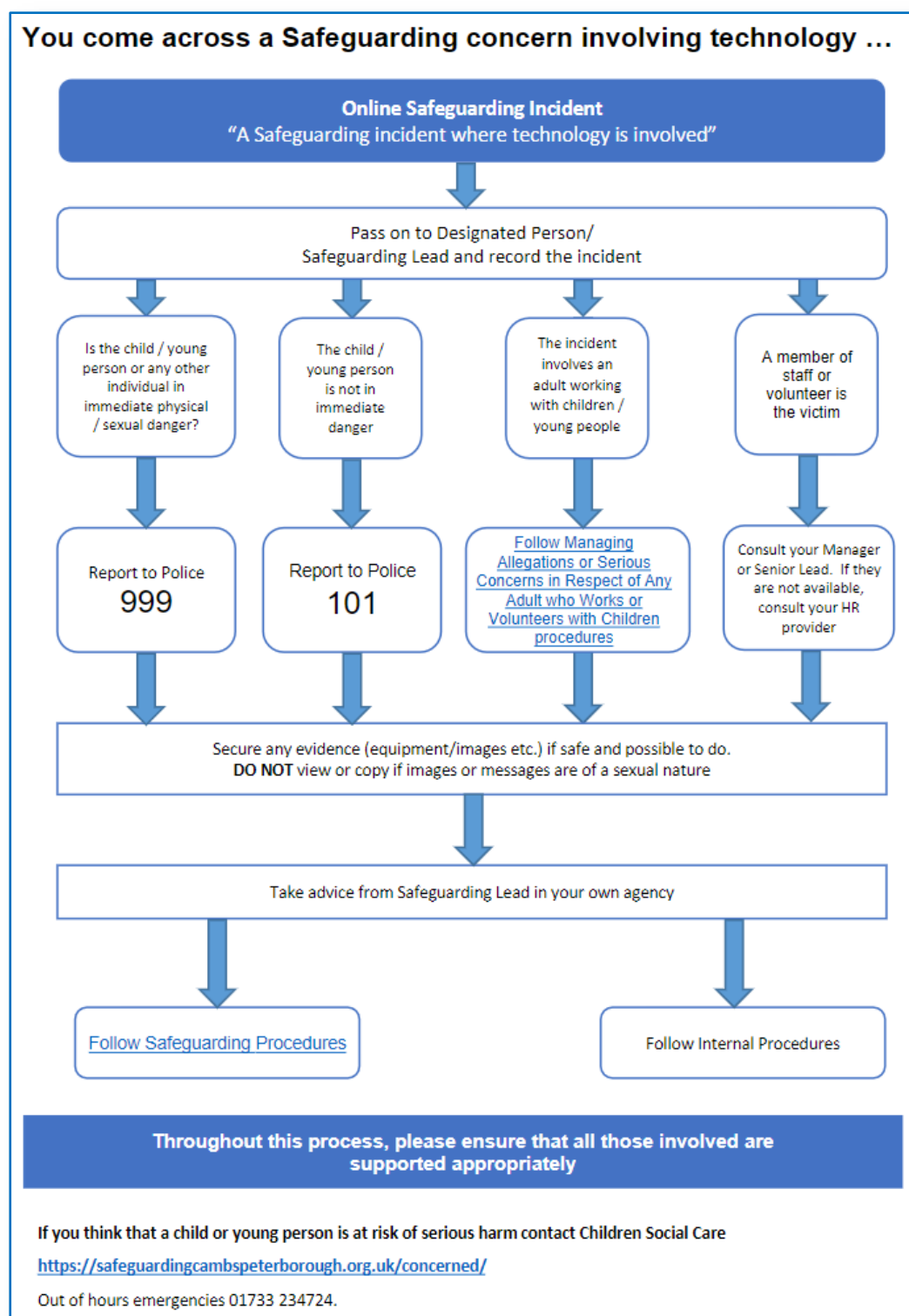
Mrs Simpkin Smith (Headteacher)

Signed:

Mr Nick Moir (Chair of Governors)

Appendix 1:

Where the school suspects that an incident may constitute a Safeguarding issue, the usual Safeguarding procedures will be followed. This process is illustrated in the diagram below.



Appendix 2:

Child Acceptable User Agreement KS2



Teversham CE Primary Child User Agreement (KS2)

Being Safe Online

- I will never share my passwords or usernames with anyone except a trusted adult.
- I will only use the websites or apps my teacher tells me to use.
- I will ask for help if I am stuck, worried, or unsure.
- I will tell an adult straight away if I see something online that upsets me.
- I understand that the school can see what I have been looking at and that inappropriate searches are flagged.
- I will not take photos, videos or sound recordings of others without their permission.
- I will be kind online and treat others with respect. I will not say or send unkind messages, and I will never cyberbully anyone. If I see someone being unkind online, I will tell a trusted adult.

Looking After Equipment

- I will look after the laptops, iPads and all equipment.
- I will never carry a laptop when it is open.
- I will always walk when carrying an iPad or laptop.
- I will plug in and unplug laptops and iPads carefully, without pulling the cables hard.
- I will report any damages or faults I encounter with iPads or laptops.

Working Sensibly in Class

- I will follow the instructions given by my teacher.
- I will work sensibly with a partner, sharing and taking turns.
- I will save my work sensibly using my name.
- I will not touch anyone else's laptop or iPad without permission.
- I understand the iPads and laptops are intended for educational use.
- I will not alter any settings on the devices.
- I will shut down the laptop properly by following the steps, not by pressing the power button.

Consequences

- I understand that an adult has the right to take appropriate actions against me, such as having equipment removed, having to work with an adult, or having discussions with my parents if I fail to follow these rules.

Pupil Agreement

I have read (or someone has read to me) this agreement. I understand it, and I promise to follow these rules whenever I use school technology.

Name: _____

Class: _____

Pupil Signature: _____

Date: _____

Appendix 3:

Child Acceptable User Agreement KS1



Teversham CE Primary Child User Agreement (KS1)

Being Safe

- I will keep my password safe and not tell anyone except my teacher or a trusted adult.
- I will tell an adult if I see something that makes me sad, worried or confused.
- I will ask for help if I don't know what to do.
- I will be kind when I am online. I will use kind words, and I will not say or send anything that could hurt someone's feelings. I will never be unkind or bully anyone online, and if I see something unkind, I will tell a trusted adult.

Looking After Our Devices

- I will carry iPads and laptops carefully and walk with them.
- I will never carry a laptop when it is open.
- I will be gentle when plugging in and unplugging the cables. I won't pull the wires.
- I will look after the iPads and laptops and keep them safe.
- I will tell an adult straight away if something is broken or not working.

Listening and Following Instructions

- I will only go on the apps or websites my teacher says.
- I will follow all instructions from my teacher.
- I will not change any settings on the iPads or laptops.

Working With Others

- I will work kindly and sensibly with a partner.
- I will not touch anyone else's iPad or laptop unless they say I can.
- I will not take photos, videos or sound recordings of others without their permission.

Using Technology the Right Way

- I understand the iPads and laptops are for learning.
- I will save my work using my name so I can find it again.
- I know the school can see what I have looked at.

- I will shut down laptops properly and not press the power button unless told to.

Consequences

- I understand that an adult may take action, such as not letting me use the device, working with an adult, or talking to my parents, if I do not follow these rules.

My Agreement

I have listened to these rules and I promise to try my best to follow them when using technology at school.

Class: _____

Signed: _____

Appendix 3:

Parent Acceptable User Agreement



Teversham CE Primary Parent User Agreement

1. Purpose of this Agreement

At Teversham CE Primary School, online safety is a core part of safeguarding. Parents and carers play a crucial role in supporting children to use technology safely at home and in partnership with the school. This agreement outlines expectations for parents/carers to help keep children safe online, in line with *Keeping Children Safe in Education (KCSIE)* and the school's Online Safety Policy (see website).

Parents are asked to read this agreement carefully and discuss its contents with their child, alongside the child-friendly KS1 or KS2 User Agreement (see appendices)

2. Parent / Carer Responsibilities

Supporting Safe and Responsible Use

I will:

- Support my child to follow their **Child User Agreement** (KS1 or KS2) and remind them of the school's rules for responsible technology use.
- Encourage my child to speak to a trusted adult (at home or school) if something online worries or upsets them.
- Remind my child never to share personal information, logins, or passwords except with trusted adults, in line with school expectations.
- Teach my child to be kind, respectful and safe online, consistent with the school's emphasis on positive online conduct.

Working in Partnership With the School

I understand that:

- The school uses **monitoring systems, filtering, supervision and alerts** to help keep children safe online when using school devices and systems.
- The school may contact parents if concerns arise regarding a child's online behaviour, searches, communication or activity, as outlined in the Online Safety Policy.
- The school may apply sanctions if rules are not followed, including restricted access to devices or platforms.

- Online behaviours that occur outside school, but impact the school community (e.g. cyberbullying), may still result in action by the school in line with legal powers and safeguarding duties.

3. Use of Technology at Home

To support my child's safety online, I will:

- Monitor my child's use of the internet, social media, online games and messaging apps according to their age and maturity.
- Ensure my child only accesses age-appropriate websites, games, and platforms, consistent with the school's risk-based approach to safe content.
- Ensure parental controls, privacy settings and appropriate filters are in place on devices used at home.
- Teach my child to recognise risks associated with **Content, Contact, Conduct and Commerce**, as identified in KCSIE and the school's policy (including harmful content, scams, grooming, cyberbullying, misinformation and excessive use).

4. Communication and Digital Etiquette

I agree to:

- Communicate respectfully with staff via approved school channels.
- Avoid sharing sensitive information or concerns publicly on social media; instead speak directly to the school.
- Use school-provided online platforms appropriately and support my child to do the same.

5. Mobile Phones and Devices

I understand that:

- Children are **not permitted to bring mobile phones to school**, unless agreed with the Headteacher, in line with the Online Safety Policy.
- Any approved mobile phones must be handed into the office or class teacher on arrival at school (unless required for monitored medical purposes) and these will be locked away for the school day.
- Smart watches with internet, messaging or camera functions must **not** be used during the school day unless agreed by the school.

6. Images, Videos and Online Sharing

I agree to:

- Respect the school's guidance on photography and video, particularly at school events.
- Not share images of other children from school events online, in line with safeguarding responsibilities articulated in the school's policies.

7. Reporting Concerns

I will:

- Contact the school immediately if I become aware of a safeguarding concern, online risk, or inappropriate behaviour involving any child.
- Support the school in following appropriate safeguarding procedures, as outlined in the Online Safety Policy.

8. Agreement

Parent / Carer Name: _____

Child's Name: _____

Class: _____

Signature: _____

Date: _____



Appendix 4:

Staff Acceptable User Agreement

Teversham CE Primary Staff Acceptable Use Agreement

To be read alongside:

- Online Safety Policy
- Safeguarding and Child Protection Policy
- Data Protection / GDPR Policy
- Safer Working Practices
- KCSIE statutory guidance
- Staff Code of Conduct

1. Purpose of This AUP

This Acceptable Use Policy establishes the expectations, responsibilities, and safe working practices required of all staff when using digital technologies—both school-owned and personal—while working with or around pupils.

It ensures compliance with current safeguarding guidance, including the proposed updates in **KCSIE 2026**, which emphasise:

- clarity of staff responsibilities
- strengthened handling of **self-generated intimate images (including AI-generated)**
- emerging online risks and harmful ideologies
- information security and access management

It also reflects our school's Online Safety Policy, including filtering, monitoring, password use, staff training, and safe use of devices.

2. Scope

This AUP applies to:

- All staff (teaching, support, admin, peripatetic, supply)
- Volunteers, governors, trainees and contractors using school systems
- All devices and systems used for school business, including:

- School laptops, desktops, tablets, cameras
- Cloud systems (Microsoft 365, MIS, storage platforms)
- School email and communication tools (Teams, internal email)
- Personal devices used to access any school information
- School social media platforms and website content

3. Key Principles

Staff must ensure that their use of technology:

- ✓ protects pupils from harm
- ✓ protects themselves from allegations
- ✓ maintains the security of school systems and data
- ✓ models safe and responsible digital behaviour

Our school's Online Safety Policy emphasises that **online safety is primarily a safeguarding issue**, not a technical one. Staff therefore hold shared responsibility for enforcing safe practice and reporting concerns.

4. Safe Use of School Devices and Systems

4.1 Access and accounts

- Staff must use **individual, password-protected logins** for the network, cloud services, and MIS systems, as outlined in the school policy.
- Passwords must remain confidential and changed if compromised.
- Staff must **never share login credentials** with pupils, colleagues, or visitors.
- School systems must not be accessed by unapproved devices.

4.2 Use of personal devices

- Personal devices must **not be connected** to the school's wireless network unless explicitly permitted (e.g., guest access).
- Sensitive or identifiable pupil data must **not be stored** on personal devices unless encrypted and authorised.
- Staff must not use personal messaging apps or social media to communicate with pupils.

4.3 Data protection

- Staff must follow GDPR and our school's Data Protection Policy.
- Only secure school systems may be used to store pupil data.

- Personal emails must NOT be used for school business.

4.4 Monitoring

- Staff use of the internet and online systems may be monitored in line with the school's Online Safety Policy.
- Monitoring systems automatically flag safeguarding-risk behaviour on Teams or web activity.

5. Safe Working With Pupils Online

5.1 Supervision and usage

- Staff must supervise pupils using online technologies as required in the Online Safety Policy.
- Staff are responsible for ensuring pupils access appropriate content through filtered systems.

5.2 Communication with pupils

- All digital communication with pupils (e.g., Teams messages, feedback, emails) must be **professional, transparent, and school-based**.
- Staff must not initiate or accept social media contact with pupils or former pupils under 18.

5.3 Online teaching / remote learning

If remote learning occurs:

- Only school-approved platforms may be used.
- Staff must ensure neutral backgrounds, appropriate dress, and no personal information visible.
- Lessons should be recorded or logged according to safeguarding procedures.

6. Preventing and Managing Online Risks

6.1 Prohibited behaviours

Staff must NOT:

- Access or attempt to access harmful, extremist, illegal, or inappropriate content.
- Create, store, or share **self-generated intimate images**, including those produced with AI—highlighted as a risk area in KCSIE 2026.
- Engage in online behaviour that could be perceived as bullying, discriminatory, or unprofessional.

- Download unapproved software or bypass filtering/monitoring.

6.2 Managing emerging online risks

Staff must be alert to:

- misogynistic, extremist, or harmful online ideologies influencing pupils
- AI-generated content posing risks to pupil identity or wellbeing
- mobile data bypassing filtering systems (referenced in KCSIE)

Any concerns must be logged following safeguarding procedures.

7. Use of Mobile Phones and Personal Smart Tech

In line with our school policy:

- Staff personal phones must be kept out of sight and not used in teaching areas unless authorised for safety or emergency use.
- Staff must NEVER photograph pupils with personal devices.
- Pupils' mobile phone rules (hand-in system, exceptions for medical needs) must be enforced consistently.

8. Social Media, Public Communication, and School Representation

- Staff must not identify or discuss pupils, colleagues, or school matters on personal social media.
- School social media platforms must only be used by authorised members of staff.
- Staff must follow the Online Safety Policy guidance on ensuring pupils **cannot be individually identified** on the school website.

9. Responding to Online Safety Concerns

Staff must follow our school's safeguarding flowchart (see appendix 1) when:

- a pupil reports an online concern
- staff witness or suspect harmful online behaviour
- content is illegal, inappropriate, or places a child at risk

KCSIE emphasises clarity on early help, risk indicators, and consistent management of safeguarding concerns.

In line with our school policy:

- Internal sanctions, account restrictions, and parental involvement may be used.
- The school may involve external agencies, including the police, for serious incidents.
- Staff must NOT delete or share potentially harmful content unless instructed by DSL.

10. Safe Handling of Digital Evidence

- Staff must immediately report concerns to the DSL.
- No screenshots, forwarding, or deletion unless directed by safeguarding procedures.
- Devices belonging to pupils may be searched only under lawful conditions (Education Act 2011) and with reference to safeguarding guidance.

11. Staff Responsibilities and Compliance

All staff must:

- Read and sign this AUP annually
- Complete safeguarding and online safety training
- Promote digital resilience and safe online habits in pupils
- Maintain professional standards in all digital interactions
- Report breaches or risks without delay

Failure to follow this AUP may result in:

- disciplinary action
- revocation of system access
- safeguarding investigation
- involvement of external agencies

Name: _____

Signed: _____

Dated: _____

