



CHILTON FOLIAT CofE VA PRIMARY SCHOOL



Our School Christian Vision

With thankfulness, courage and love,
we strive to improve heart and mind.

At Chilton Foliat Primary School we honour our educational heritage, supported by a strong Christian ethos. We strive to provide a diverse education that inspires children to develop a **thirst for knowledge**. This is delivered in a safe, thoughtful and nurturing environment promoting self-discipline, motivation and excellence in all that we do. We encourage strong partnerships and inclusive relationships amongst pupils, parents, carers, staff and the wider community. Our children leave Chilton Foliat Primary School with a deep understanding of the impact of living out our school Christian vision and values. As a result, they are well-rounded, confident and able to contribute positively to a wider community. They want to continue to **thirst for knowledge** and strive to improve **heart** and **mind** enjoying a diverse curriculum in their next educational setting.

Online Safety Policy

Date Reviewed	September 2025
Review Period	Annually /2 Yearly/Readopted/Other
Review Body	Headteacher/DPA and Standards Committee

With thankfulness, courage and love, we strive to improve heart and mind

Jesus said, "Everyone who drinks of this water will be thirsty again, but whoever drinks the water I give him will never thirst". John 4:13



CHILTON CoFE VA FOLIAT PRIMARY SCHOOL

Key Personnel			
Role	Name	Tel:	Email
Headteacher	Katie Turner	01488 682630	head@chiltonfoliat.wilts.sch.uk
Online Safety Lead	Katie Turner	01488 682630	head@chiltonfoliat.wilts.sch.uk
Designated Safeguarding Lead (DSL)	Katie Turner	01488 682630	head@chiltonfoliat.wilts.sch.uk
Deputy DSL (DDSL)	Emma Pinnegar	01488 682630	epinnegar@chiltonfoliat.wilts.sch.uk
Nominated Governor	Sam Wolcough	01488 682630	Chair@chiltonfoliat.wilts.sch.uk
Chair of Governors	Sam Wolcough	01488 682630	chair@chiltonfoliat.wilts.sch.uk



Scope of the Online Safety Policy

This Online Safety Policy outlines the commitment of Chilton Foliat Primary School to safeguard members of our school community online in accordance with statutory guidance and best practice.

This Online Safety Policy applies to all members of the school community (including staff, learners, governors, volunteers, parents and carers, visitors, community users) who have access to and are users of school digital systems, both in and out of the school. It also applies to the use of personal digital technology on the school site (where allowed).

Chilton Foliat Primary School will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that take place out of school.

This policy also covers the safe and appropriate use of emerging digital technologies, including AI-based tools, and recognises the growing risks of misinformation, disinformation and manipulated digital content.

Aims

Chilton Foliat Primary School aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors.
- Deliver an effective and empowering approach to online safety, ensuring the whole school community can use technology safely, responsibly and confidently, including mobile and smart technologies.
- Establish clear mechanisms to identify, intervene and escalate concerns, ensuring incidents are managed promptly, proportionately and in accordance with safeguarding procedures.
- Ensure compliance with the DfE Filtering and Monitoring Standards, including the *annual use of the DfE self-assessment tool* to review system effectiveness and identify areas for improvement.
- Ensure cyber-security measures meet the DfE Cyber Security Standards for schools, including:
 - regular cyber-security training for all members of staff
 - secure and resilient digital backups
 - a clearly defined and tested cyber-incident response plan
- Promote safe, responsible and ethical use of emerging technologies, including AI-based tools, digital communication platforms and online learning systems.
- Support pupils in recognising and responding to online risks, including misinformation, disinformation, digital manipulation and other new or developing online harms.



CHILTON CoFE VA FOLIAT PRIMARY SCHOOL

- Strengthen our partnership with parents and carers, providing guidance and resources to help them keep children safe online at home and in the wider digital environment.

The 4 key categories of risk

Our approach to online safety is based on the Department for Education's four categories of online risk. These categories help us identify, teach about and respond to the digital harms that children may encounter both in and beyond school.

1. Content — what children may see

Children may be exposed to illegal, inappropriate or harmful material online. This includes, but is not limited to:

- Pornographic or sexualised content
- Self-harm, suicide or disordered eating content
- Violence or extremism, including radicalisation materials
- Hate content such as racism, misogyny or antisemitism
- Misinformation, disinformation and conspiracy theories that may mislead, manipulate or distress pupils
- AI-generated or digitally manipulated media (e.g., deepfakes) that can cause confusion, reputational harm or emotional distress
- Fake news and misleading "clickbait" content designed to influence behaviour

We teach pupils how to think critically about what they see online and how to identify when content may be false, harmful or unsafe.

2. Contact — who children may interact with

Children may be subjected to harmful online interactions, such as:

- Grooming
- Coercion, blackmail or manipulation
- Peer-to-peer pressure or harmful influence
- Unwanted contact from strangers
- Adults posing as children or young people
- Commercial advertising targeted at children

We ensure pupils know how to recognise unsafe contact and where to go for support.

3. Conduct — how children may behave online

Children may behave in ways that increase risk or cause harm to themselves or others, such as:

- Making, sending or receiving explicit or sexualised images (e.g., consensual or non-consensual sharing of nudes and semi-nudes)
- Sharing harmful or inappropriate images or videos



CHILTON CofE VA FOLIAT PRIMARY SCHOOL

- Cyber-bullying, harassment or online abuse
- Aggressive, rude or discriminatory language
- Impersonating others or identity misuse
- Sharing personal information unsafely

We support pupils in understanding respectful online behaviour and the long-term impact of their digital actions.

4. Commerce — financial and commercial risks

Children may be exposed to online financial risks such as:

- Online scams and fraud
- Phishing attempts
- In-app purchases and micro-transactions
- Gambling or games designed with gambling-like features
- Illegal or unsafe commercial advertising

We teach pupils to make informed choices online and recognise when financial activity may be unsafe or exploitative.

Legislation and Guidance

This Online Safety Policy is based on, and must be read alongside, current statutory safeguarding legislation and national guidance. It reflects the legal duties placed on schools and the expectations set out by the Department for Education (DfE), the Home Office and other statutory bodies.

Statutory Guidance

This policy is underpinned by the following statutory documents:

- Keeping Children Safe in Education (KCSIE) 2025 – the core safeguarding guidance for all schools and colleges in England. It sets out the legal duties to safeguard and promote the welfare of children, including updated expectations around online safety, AI-related risks, misinformation/disinformation, filtering & monitoring, cyber security, attendance, and safeguarding responsibilities relating to children in kinship care.
- Working Together to Improve School Attendance (2024–25) – now recognised in KCSIE 2025 as *statutory guidance*; schools must integrate attendance processes with safeguarding procedures, ensuring early identification and escalation of attendance-related risks.
- Education Act 2002 – Section 175 requiring schools to safeguard and promote the welfare of pupils.
- Education Act 2011 – giving staff powers to search for and delete inappropriate digital content.



CHILTON CoFE VA FOLIAT PRIMARY SCHOOL

- Equality Act 2010 – duties relating to discrimination, harassment and victimisation.
- Prevent Duty Guidance – requiring schools to prevent children from being drawn into extremism.
- Searching, Screening and Confiscation (DfE) – setting out lawful procedures for examining devices.

DfE Digital and Technology Standards

To meet statutory safeguarding obligations, this policy incorporates requirements from the DfE's Digital and Technology Standards, including:

Filtering and Monitoring Standards (DfE)

Schools must have effective filtering and monitoring to protect users from illegal, inappropriate and harmful content, including misinformation, disinformation, conspiracy theories, radicalisation content, self-harm materials and AI-generated harmful content. These standards require schools to:

- Assign appropriate roles and responsibilities
- Review filtering and monitoring provision at least annually
- Ensure filtering does not excessively restrict teaching
- Use the DfE's self-assessment tool to evaluate compliance and improve practice

Cyber Security Standards (2025)

Schools must take active steps to improve cyber resilience, including:

- Staff cyber-security training
- Tested and reliable backup systems
- A clear cyber-incident response plan
- Strong password and access control measures
- Regular patching and secure system configurations

These expectations are essential because cyber incidents can compromise safeguarding data, disrupt education, and expose sensitive information.

Policy and leadership

Responsibilities

Online safety is a shared responsibility. Every member of the school community—staff, governors, pupils, parents, volunteers and external providers—has a role in promoting safe, responsible and respectful use of technology. Effective safeguarding depends on collaboration, clear communication and a commitment to reporting concerns promptly.



CHILTON CofE VA FOLIAT PRIMARY SCHOOL

The following outlines the roles and responsibilities within Chilton Foliat CofE VA Primary School.

The Governing Body

The governing body holds overall responsibility for ensuring that online safety is embedded within the school's safeguarding framework. Governors must ensure that the school:

- Has appropriate, effective policies covering online safety, filtering, monitoring and cyber security.
- Is compliant with Keeping Children Safe in Education (KCSIE) 2025 expectations, including misinformation, disinformation, AI-related risks, attendance safeguarding and responsibilities to children in kinship care.
- Reviews filtering and monitoring arrangements at least annually, using the DfE self-assessment tool, and receives regular safeguarding reports from the DSL.
- Ensures filtering systems protect pupils from illegal, inappropriate and harmful content, while avoiding over-blocking that may restrict teaching and learning.
- Embeds a whole-school approach where online safety is a continuous theme across policies, leadership discussions and curriculum planning.
- Ensures that safeguarding, including online safety, is adapted for vulnerable pupils, including those with SEND, children in care and children in kinship care.

All governors will:

- Read and understand this policy and related safeguarding documents.
- Adhere to the Acceptable Use Policy (AUP) for staff/governors/visitors.
- Ensure provision is made for staff training, leadership oversight and appropriate technical support.

Headteacher

The Headteacher has strategic responsibility for ensuring the safety and wellbeing of the school community, including online safety. They will:

- Promote a strong safeguarding culture where safe digital practice is understood and prioritised.
- Ensure that day-to-day responsibility for online safety is delegated to the DSL, while remaining fully informed and accountable.
- Ensure procedures are in place for managing allegations involving misuse of technology by staff, including rapid escalation for serious online safety concerns.
- Ensure the DSL, Online Safety Lead, IT provider and relevant staff receive appropriate and regularly updated training, including risks related to AI, digital manipulation, online harms and cyber-security.
- Oversee compliance with DfE Filtering & Monitoring Standards and Cyber Security Standards, ensuring annual review and improvement.



Designated Safeguarding Lead (DSL)

The DSL takes lead responsibility for online safety, supported by the DDSLs. The DSL will:

- Ensure consistent implementation of this policy across the school.
- Oversee and respond to all online safety concerns, ensuring incidents are recorded, analysed and managed according to safeguarding procedures.
- Liaise with external agencies (police, LA, CEOP, social care, Prevent partners and technical support services) as required.
- Ensure cyber-bullying incidents are recorded and addressed in line with school behaviour and anti-bullying policies.
- Maintain the school's online safety log (Appendix 6) and ensure patterns or emerging risks are reviewed.
- Provide regular safeguarding reports to the Headteacher and governing body, including updates on filtering and monitoring alerts.
- Lead on the creation, review and evaluation of online safety policies, technical standards and acceptable use agreements.
- Deliver or commission high-quality staff training, including:
 - online harms and digital behaviours
 - misinformation and disinformation
 - AI-related risks and manipulated media
 - cyber-security awareness
 - harmful online trends, grooming behaviours and harmful content
- Work with the Virtual School Head on safeguarding for children in care and children in kinship care, as recognised in KCSIE 2025.
- Understand and act on the links between online behaviours and attendance-related safeguarding risks.

IT Provider

The IT Provider/technical staff will:

- Follow the school's Online Safety Policy and Technical Security Policy.
- Maintain secure technical infrastructure that protects against misuse, attack and data compromise.
- Ensure the school meets DfE Filtering & Monitoring Standards, including safe configuration, annual review and appropriate escalation of alerts.
- Maintain effective control of user access rights, devices and digital services.
- Keep up to date with technical developments and emerging online risks, informing the DSL and Headteacher of relevant changes.
- Monitor technology use and promptly report concerns or attempted misuse for appropriate action.
- Support the school in meeting DfE Cyber Security Standards, including secure backups, patching, system resilience and cyber-incident response planning.



All Staff and Volunteers

All staff—including supply staff, peripatetic staff, agency workers, contractors and volunteers—must:

- Read, understand and comply with this Online Safety Policy.
- Follow the Acceptable Use Agreement for staff ([Appendix 3 and 4](#)).
- Model safe, responsible and respectful use of technology.
- Immediately report online safety concerns, including cyber-bullying, harmful content, device misuse or safeguarding worries.
- Record incidents in line with the school's procedures ([Appendix 6](#)).
- Support pupils to follow the pupil Acceptable Use Agreements ([Appendix 1 and 2](#)).
- Respond appropriately to all concerns involving sexual harassment, harmful sexual behaviour or online sexual content, maintaining an attitude that “it could happen here.”
- Be vigilant to risks including:
 - grooming
 - misinformation/disinformation
 - AI-generated harmful content
 - manipulative online contact
 - unsafe conduct
 - commercial exploitation

Staff must never use personal devices to photograph pupils or store personal data.

Class Teachers

Class teachers must:

- Deliver planned online safety education through:
 - PSHE
 - Computing
 - Assemblies and themed safeguarding weeks
 - Pastoral curriculum
 - National initiatives (e.g., Safer Internet Day, Anti-Bullying Week)
- Reinforce safe and respectful online behaviours across all subjects where technology is used.
- Adapt teaching to meet the needs of vulnerable pupils, including those with SEND.
- Encourage pupils to report online concerns and teach them how to seek help safely.
- Work with the DSL to identify and support pupils at risk of online harm.

Key Stage 1

In Key Stage 1, pupils will be taught to:

- Use technology safely and respectfully, understanding the importance of being kind and considerate online.



CHILTON CoFE VA FOLIAT PRIMARY SCHOOL

- Keep personal information private, including names, addresses, school details, images and passwords.
- Recognise when something online makes them feel worried, confused or upset, and understand that they must always tell a trusted adult.
- Identify where to go for help and support if they are concerned about content or contact on the internet or other online technologies.
- Begin to understand that not everything they see online is real, and that some information may be wrong, confusing or misleading.

Key Stage 2

In Key Stage 2, pupils will be taught to:

- Use technology safely, respectfully and responsibly, showing consideration for others in all digital interactions.
- Recognise acceptable and unacceptable online behaviour, including what constitutes bullying, unkindness, manipulation or inappropriate content.
- Understand how to protect personal information, including what is safe or unsafe to share.
- Identify a range of ways to report concerns about content, contact or conduct, both inside and outside school.
- Begin to evaluate the trustworthiness and reliability of online information, including recognising misinformation and disinformation.
- Develop awareness of AI-generated or digitally manipulated content, understanding that things online can be edited or artificially created.

By the end of primary school, pupils will know:

Understanding People and Relationships Online

- 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, kindness and boundaries, even when communication is anonymous.
- How to respond safely and appropriately to unknown adults online, including never meeting someone they have only spoken to online without a trusted adult present.

Recognising and Responding to Risk

- The rules and principles for keeping safe online, including how to recognise risks, harmful content and unsafe contact.
- How to report concerns using clear, age-appropriate routes, both in school and externally (e.g., speaking to a trusted adult, reporting on a website or app).
- That online information can be true, false, misleading or incomplete, and how to question and check sources.

Digital Resilience and Critical Thinking

- How to critically consider online friendships and information, including the risks associated with interacting with people they have never met.
- How information and data is shared, tracked and used online, including the concept of digital footprints.



CHILTON CoFE VA FOLIAT PRIMARY SCHOOL

- That content online, including images and videos, can be edited, altered or artificially generated (including AI-generated content or deepfakes).

Healthy Boundaries

- What sorts of boundaries are appropriate in friendships and communications, including in digital contexts (e.g., group chats, messaging apps, gaming).
- How to respond safely if they see something upsetting or if someone online acts in a way that makes them feel uncomfortable, scared or pressured.

Parents and Carers

Parents and carers play a vital role in supporting their children to become safe, responsible and confident users of technology. Chilton Foliat Primary School values strong partnerships with families and recognises that online safety is most effective when school and home work together.

The school will take every opportunity to help parents and carers understand online safety risks and how to support their children's digital wellbeing. This includes:

- Publishing this Online Safety Policy and related guidance on the school website.
- Seeking and managing photographic and digital consent in line with safeguarding and data protection requirements.
- Providing information through newsletters, workshops, school events and online platforms about national and local online safety initiatives, including new and emerging online risks (e.g., misinformation, disinformation, scams, AI-generated content).
- Sharing age-appropriate guidance to help families support safe use of devices, social media, gaming platforms and online communication tools at home.

Parents and carers are expected to:

- Raise any concerns, queries or observations about online safety with a member of staff or the Headteacher as soon as they arise.
- Ensure their child has read, understood and agreed to the relevant Acceptable Use Agreement (**Appendices 1 and 2**), and support the school in upholding these expectations.
- Model safe and respectful digital behaviour at home and help reinforce messages about privacy, reliability of information, and safe online conduct.

To further support families, parents and carers are encouraged to seek additional online safety advice from reputable national organisations.

The school remains committed to working closely with parents and carers to promote a consistent approach to online safety and to ensure pupils are well supported in navigating an increasingly complex digital world.



Learners

Learners are active participants in creating a safe and respectful online environment. All pupils are expected to understand and follow the school's expectations for responsible use of technology and to seek help whenever they feel unsure or unsafe.

All learners:

- Are responsible for using the school's digital technology systems safely, respectfully and in line with the Learner Acceptable Use Agreement and this Online Safety Policy.
- Must read, understand and agree to the Acceptable Use Agreements (Appendices 1 and 2) appropriate to their age, and follow these expectations at all times.
- Should immediately report abuse, misuse or access to inappropriate materials, whether this affects them or someone else. Pupils will be taught clear, age-appropriate ways to report concerns and get support.
- Should know what to do if they feel worried, unsafe or vulnerable online, including how to seek help from a trusted adult in school or at home.
- Must understand the importance of safe digital behaviours beyond school, recognising that their online actions outside school hours can still affect themselves, others and the wider school community.
- Should learn to recognise when online information may be false, misleading or harmful, and be supported to develop critical thinking skills to navigate an increasingly complex digital world.
- Should understand that the school's expectations for conduct apply both in and out of school, including behaviour on messaging platforms, gaming environments and social media when it relates to their membership of the school.

Cyber-bullying

Definition

Cyber-bullying is bullying that takes place through digital technology. It can occur on social networking sites, messaging apps, gaming platforms, email or any online space where communication occurs. As with all forms of bullying, cyber-bullying involves:

- Repeated, intentional harm
- A power imbalance
- Actions by an individual or group towards another individual or group

Examples include sending threatening or upsetting messages, posting or sharing harmful images or content, impersonation, exclusion from online groups, or spreading rumours digitally.



CHILTON CoFE VA FOLIAT PRIMARY SCHOOL

Cyber-bullying may also overlap with peer-on-peer abuse, harassment, online sexual harassment or sharing of sexual images.

Preventing Cyber-Bullying

Chilton Foliat Primary School takes proactive steps to prevent cyber-bullying by:

- Teaching pupils what cyber-bullying is, how it happens, and how to recognise when they or someone else is being harmed.
- Providing age-appropriate online safety education across the curriculum (Computing, PSHE, assemblies and pastoral work).
- Encouraging pupils to speak up if something online makes them uncomfortable, anxious or unsafe.
- Creating a safe culture where pupils know that any concerns will be taken seriously and dealt with promptly.
- Supporting safe, respectful and responsible online interactions at all times.
- Helping pupils understand the emotional impact of online behaviour and how to show empathy online.
- Ensuring pupils understand the importance of not participating in gossip, forwarding hurtful messages, or sharing harmful or inappropriate content.

Recognising Cyber-Bullying

Cyber-bullying can occur:

- During school hours
- Outside school hours
- On personal or school-managed devices
- In group chats, gaming platforms or social media accounts
- Publicly or privately

The school recognises that cyber-bullying often takes place outside school, but may have a significant impact inside school, affecting wellbeing, attendance or safety. When this happens, the school will respond in line with safeguarding and behaviour policies.

Reporting Cyber-Bullying

Pupils are encouraged to report cyber-bullying immediately to:

- A trusted adult in school
- Their class teacher



CHILTON CofE VA FOLIAT PRIMARY SCHOOL

- The DSL or a DDSL
- Any member of staff they feel comfortable speaking to

Parents and carers are also encouraged to report concerns directly to the school as soon as possible.

All staff must respond to reports of cyber-bullying and escalate them to the DSL in line with safeguarding procedures.

Responding to Cyber-Bullying

When a cyber-bullying concern is raised, the school will:

1. Take the report seriously and reassure the child.
2. Record the incident using the school's online safety incident log (Appendix 6).
3. Investigate appropriately, involving pastoral staff, class teachers and the DSL as required.
4. Follow the behaviour policy to determine proportionate and appropriate actions.
5. Support the pupil(s) affected, including emotional support and restorative approaches where appropriate.
6. Work with parents and carers to ensure consistent messaging and support at home.
7. Involve external agencies if needed, such as the police, particularly if the incident involves illegal content (e.g., threats, harassment, or sharing of sexual images).

The school will take reasonable steps to ensure harmful material is contained, including working with platforms to remove content where appropriate.

Staff Training and Awareness

All staff, governors and volunteers receive training on:

- What cyber-bullying looks like
- How to report it
- How to support pupils affected
- Online harms including misinformation, digital manipulation and harmful trends
- How online behaviour can link to broader safeguarding concerns, including attendance and wellbeing

Training ensures a consistent whole-school approach to identifying, preventing and responding to cyber-bullying.



Acceptable Use of the internet in school

Chilton Foliat Primary School is committed to ensuring that all members of the school community use technology safely, responsibly and respectfully. Clear expectations around the use of ICT systems, devices and the internet ensure that everyone understands their safeguarding responsibilities.

Staff, Volunteers and Governors

All staff, including supply staff, governors, volunteers, contractors and agency workers, are required to:

- **Read, understand and sign** the school's Acceptable Use Agreements (Appendices 3 and 4) before accessing school ICT systems or using school devices.
- Always Follow the Online Safety Policy and wider safeguarding procedures.
- Use school systems and internet access solely for educational purposes or for fulfilling the professional duties of their role.
- Model safe, respectful and lawful online behaviour.

Visitors

Visitors who require access to the school's network or devices will be asked to read and agree to the relevant Acceptable Use expectations before being permitted access. Temporary access will be monitored and restricted as appropriate.

Parents and Carers

All parents and carers will:

- Receive a copy of the school's Online Safety Policy.
- Be expected to read, understand and support the expectations within it.
- Support their children in following the pupil Acceptable Use Agreements.
- Reinforce safe and respectful online behaviour at home.

Where appropriate, **Key Stage 2 pupils** will read and sign their own Acceptable Use Agreement (Appendix 2), with parents/carers supporting this process.

Families joining Chilton Foliat Primary School will receive the Online Safety Policy and the relevant Acceptable Use Agreements as part of the admissions process, which must be completed and returned before ICT access is granted.

Appropriate Use of the School Internet

- Use of the school's internet and digital systems must be for educational purposes only, or for the completion of duties linked to a member of staff's role.



CHILTON CoFE VA FOLIAT PRIMARY SCHOOL

- Personal use of school ICT systems is not permitted unless authorised and must never compromise safeguarding, data security or school operations.
- Pupils are only permitted to access the internet under appropriate supervision.

Monitoring and Oversight

To safeguard users and maintain the security of our digital environment, the school will:

- Monitor websites and online content accessed via the school network.
- Record and review online activity where appropriate, in line with filtering and monitoring standards.
- Investigate concerns or breaches promptly, involving the DSL, Headteacher or IT provider where necessary.

Monitoring will always be undertaken in a way that is fair, proportionate and consistent with safeguarding, data protection and privacy requirements.

Pupils using mobile devices in school

Chilton Foliat Primary School is committed to ensuring that pupils can learn in a safe, calm and focused environment. Personal mobile or smart devices can present safeguarding, distraction and data-protection risks; therefore, their use in school is tightly controlled.

General Expectations

- Pupils are not permitted to bring personal mobile phones or any internet-enabled smart devices (e.g., smart watches, fitness trackers, tablets) onto the school site unless exceptional circumstances have been agreed in advance by the Headteacher.
- Examples of prohibited devices include (but are not limited to):
 - Mobile phones
 - Smart watches (including those with messaging, calling or internet functions)
 - Fitness trackers with connectivity
 - Gaming devices
 - Tablets and personal laptops

Exceptional Circumstances

In rare and exceptional circumstances—such as health, medical or safety needs—the Headteacher may grant written permission for a pupil to bring a device to school. In these cases:



CHILTON CoFE VA FOLIAT PRIMARY SCHOOL

- The device must be handed in on arrival and collected at the end of the school day.
- The device must remain switched off throughout the day and must not be used on the school premises.
- Parents and pupils must agree to follow the conditions set by the school.

Use of School-Owned Devices

Where pupils use school-owned devices (e.g., iPads, laptops):

- They must follow the pupil Acceptable Use Agreements ([Appendix 1 for EYFS/KS1](#) and [Appendix 2 for KS2](#)).
- Devices must be used only for educational purposes and under appropriate supervision.
- Any attempt to access, download or share inappropriate content is strictly prohibited and will be treated as a safeguarding concern.

Breaches of the Policy

Any breach of these expectations will result in:

- Confiscation of the device
- Contact with parents and/or carers
- Review of privileges or access to technology
- Additional actions under the Positive Behaviour Policy or Safeguarding Policy, depending on severity

Where misuse involves bullying, unsafe behaviour, or potential harm, the matter will be escalated to the DSL immediately.

Rationale for Policy

This approach is in place to:

- Reduce distractions during learning
- Protect pupils from online harm
- Support digital wellbeing
- Maintain a safe, orderly environment
- Prevent unauthorised recording or sharing of images
- Safeguard pupil privacy and data

Chilton Foliat Primary School remains committed to helping pupils develop healthy digital habits and responsible attitudes towards the use of mobile and smart technology.

Staff using work devices outside school



CHILTON CoFE VA FOLIAT PRIMARY SCHOOL

Chilton Foliat Primary School issues staff with work devices (such as laptops and iPads) to support teaching, learning and administrative duties. When staff use these devices outside school, they must continue to uphold the highest standards of safeguarding, data protection and cyber security.

Staff must take all reasonable steps to ensure that work devices remain secure, protected and used appropriately at all times.

Security Expectations

All staff must ensure that:

- Devices are password-protected, using strong, unique passwords that are not shared with anyone.
- Automatic locking is enabled so devices lock when inactive.
- Encryption is enabled on all school-owned devices, ensuring that data cannot be accessed if a device is lost or stolen.
- Operating systems, antivirus and security updates are installed promptly when requested.
- Devices are not used by family members, including children, under any circumstances.
- Devices are stored securely when not in use and never left unattended where loss or damage could occur.

Use of Devices

When using a work device outside school, staff must:

- Use the device solely for work-related activities.
- Never store or transfer pupil data on a personal device or unapproved platform.
- Use only school-approved software, apps and cloud services (e.g., school-managed email, school-approved storage solutions).
- Avoid connecting to unsafe or public Wi-Fi networks for work purposes, unless using a secure connection or VPN.
- Ensure that any digital images or videos of pupils are taken only on school devices and remain on those devices or approved systems.

Staff must never use personal devices to store, photograph or communicate with pupils.

Reporting Concerns

Staff must immediately report:

- Lost, damaged or stolen devices
- Any suspected data breach



CHILTON CoE VA FOLIAT PRIMARY SCHOOL

- Any suspected cyber incident (e.g., unusual device activity, phishing attempts, suspicious pop-ups)
- Any access by an unauthorised person

Reports should be made to the Headteacher or the school's IT provider without delay, so that safeguarding and cyber-security procedures can be followed.

Compliance with Cyber Security Standards

In line with DfE expectations, staff must:

- Complete cyber-security training provided by the school.
- Understand and follow the school's Cyber Response Plan.
- Support the school's compliance with DfE Cyber Security Standards by ensuring that devices are used safely and securely outside school.
- Contribute to a culture of vigilance, recognising that cyber incidents can compromise safeguarding, learning and personal data.

Consequences of Misuse

Misuse of work devices—including insecure storage, unauthorised use, inappropriate access or failure to follow this policy—may result in:

- Restriction of device access
- Further training or support
- Disciplinary action in line with the Staff Code of Conduct and Safeguarding Policy

Examining Electronic Devices

Chilton Foliat Primary School follows statutory guidance when searching, screening or examining electronic devices. The purpose of any search is to keep pupils and staff safe and to respond proportionately to safeguarding concerns.

Only authorised staff—the Headteacher, DSL or DDSL—may carry out searches of electronic devices.

When a Device May Be Searched or Confiscated

Authorised staff may search for and/or confiscate an electronic device where they have reasonable grounds to suspect that the device:

- Poses a risk to the safety of pupils or staff
- Is prohibited under the school rules
- Contains evidence relating to an offence



CHILTON CofE VA FOLIAT PRIMARY SCHOOL

The threshold for reasonable suspicion may include information shared by pupils, staff, parents or observed behaviour.

Before Conducting a Search

Before carrying out a search, the authorised staff member will:

- **Assess the urgency** of the situation, taking into account the level of risk to pupils and staff
- If not urgent, seek guidance from the Headteacher (if the Headteacher is not conducting the search)
- Explain the reason for the search to the pupil and how it will be carried out
- Give the pupil the opportunity to ask questions and seek clarification
- Seek the pupil's cooperation, recognising that a cooperative approach reduces distress and ensures procedural fairness
- Inform parents/carers, unless doing so would compromise a safeguarding concern or police involvement

All searches will be carried out with dignity, sensitivity and respect for the pupil involved.

If Inappropriate Material Is Found

If a device is found to contain inappropriate, harmful or concerning material, the Headteacher, DSL or DDSL will determine the most appropriate response. This may include:

- Following the school's Positive Behaviour Policy
- Following the Safeguarding and Child Protection Policy
- Contacting parents or carers
- Seeking advice from external agencies (e.g., the Police, MASH, Prevent Lead)

Where material places a child at risk of harm, the device and its contents will be managed as a safeguarding concern.

Deleting or Retaining Material

If staff reasonably believe that data on a device may be evidence of a criminal offence, they must not delete, alter or view the material. Instead:

- The device will be secured
- The police will be contacted as soon as reasonably practicable.

If material does not constitute evidence of an offence but poses a risk of harm, authorised staff may decide to delete the material only if:

- Its continued existence is likely to cause harm to any individual



CHILTON CoFE VA FOLIAT PRIMARY SCHOOL

- The pupil or parent refuses to delete the material themselves

A clear record of decisions and actions will be kept.

Indecent Images of Children (Nudes or Semi-Nudes)

If a staff member suspects a device contains:

- Indecent images of a child
- Nudes or semi-nudes
- Sexually explicit content involving pupils

...they must not view, forward or copy the material.

They must immediately follow the procedures outlined in the Reporting and Responding to Incidents section, including:

- Securing the device
- Referring to the DSL
- Following UKCIS *Sharing Nudes and Semi-Nudes* guidance
- Contacting police where appropriate

This approach protects pupils and staff and ensures compliance with the law.

Carrying Out Searches Safely and Lawfully

All searches must comply with:

- DfE guidance: "Searching, Screening and Confiscation"
- UKCIS guidance: "Sharing Nudes and Semi-Nudes: Advice for Education Settings"

These documents set out how searches must be conducted to protect pupils' rights, dignity and welfare.

Complaints or Concerns

Any concerns or complaints about how a search has been conducted will be managed through the school's Complaints Procedure.

Serious allegations will be escalated in line with safeguarding and staff conduct policies. Reporting and Responding

Chilton Foliat Primary School recognises that online safety incidents can occur inside and outside school and may involve pupils, staff, parents, visitors or members of the wider community. The school is committed to responding quickly, proportionately and effectively to all concerns to safeguard pupils and maintain a safe digital environment.



CHILTON CofE VA FOLIAT PRIMARY SCHOOL

Clear, consistent reporting and response procedures ensure that harmful, inappropriate or illegal online activity is identified early and managed in line with statutory safeguarding duties.

Reporting Concerns

All members of the school community—including pupils, staff, parents, volunteers and visitors—must report online safety concerns as soon as they arise. Concerns may include:

- Access to or sharing of harmful or inappropriate content
- Contact from unknown or suspicious individuals
- Cyber-bullying or peer-on-peer abuse
- Technical misuse of devices or school systems
- Online behaviour that makes someone feel worried, unsafe or vulnerable
- Potentially illegal online activity
- Harmful trends, challenges or viral content
- Misinformation, disinformation or manipulated/AI-generated content that may impact pupil safety or welfare

Reports should be made to:

- The Designated Safeguarding Lead (DSL)
- A Deputy DSL
- The Headteacher, if the concern involves staff or if escalation is required

Pupils will be taught simple, clear reporting routes and encouraged to speak to a trusted adult whenever something online feels wrong.

Immediate Response

When a concern is raised, staff will:

1. Listen, reassure and take the report seriously
 - No concern will ever be dismissed or minimised.
2. Record the concern promptly
 - Using the school's Online Safety Incident Log ([Appendix 6](#)).
3. Refer the concern to the DSL
 - Without delay, following safeguarding procedures.
4. Secure any relevant device or evidence safely
 - Without viewing or sharing any potentially illegal material.
5. Assess risk and take immediate safeguarding actions as required.

Where a child is in immediate danger, emergency services will be contacted promptly.

DSL Response and Investigation



The DSL (or DDSL) will:

- Review the incident log entry and gather appropriate information.
- Assess the level of risk, including any potential harm to individuals or groups.
- Take proportionate action in line with school safeguarding procedures.
- Contact parents/carers where appropriate, unless doing so would place a child at additional risk.
- Liaise with external agencies as needed, such as:
 - Police
 - Social care
 - CEOP
 - Prevent professionals
 - LA safeguarding teams
 - The school's IT provider

Where relevant, the DSL will also assess links between online activity and attendance-related safeguarding concerns.

Illegal or High-Risk Content

Concerns involving suspected illegal activity—including extremist content, sexual content involving children, or serious harassment—must be escalated immediately.

In these cases:

- The device must be secured but not searched by staff.
- Staff must not view, copy or share any illegal material.
- Police or external safeguarding partners will be contacted promptly.
- The DSL will follow national guidance (including UKCIS and DfE guidance).

Responding to Peer-on-Peer Online Abuse

Incidents involving peer-on-peer harm online (e.g., cyber-bullying, sharing of harmful content, coercion, online sexual harassment) will be managed in line with:

- The Safeguarding and Child Protection Policy
- The Positive Behaviour Policy
- Anti-Bullying measures
- Relevant national guidance

Support will be offered to all young people involved, including the target, the alleged perpetrator and any witnesses.

Containment of Harmful Content



CHILTON CofE VA FOLIAT PRIMARY SCHOOL

Where harmful or inappropriate content has been shared:

- The school will take reasonable steps to contain or remove the content where possible.
- The school may request takedowns from platforms or apps.
- Technical support will be sought if needed.

The focus will remain on safeguarding the child, not penalising them for reporting.

Recording and Monitoring

All incidents will be logged using the school's Online Safety Incident Log ([Appendix 6](#)), including:

- A summary of the concern
- Who raised the report
- Actions taken
- Agencies involved (if any)
- Follow-up actions and outcomes

The DSL will regularly review online safety logs to:

- Identify patterns or repeated issues
- Inform staff training
- Strengthen filtering and monitoring
- Update risk assessments and policies where necessary

Feedback and Follow-Up

Following an investigation:

- The DSL will ensure appropriate support is in place for the child or children involved.
- Parents/carers will be informed of outcomes where appropriate.
- Restorative or preventative work may be carried out with individuals or groups.
- The school may implement additional protective measures if needed (e.g., modified access, increased supervision, device restrictions).

Complaints and Escalation

If a parent, pupil or member of staff is unhappy with the handling of an incident, they may:

1. Raise their concerns with the DSL or Headteacher
2. Use the school's Complaints Procedure for further escalation



CHILTON COFE VA FOLIAT PRIMARY SCHOOL

Concerns involving staff conduct will always follow the school's Managing Allegations Policy.

Filtering and Monitoring

Chilton Foliat Primary School is committed to providing a safe online environment for pupils, staff, volunteers and visitors. Effective filtering and monitoring systems are essential to safeguarding children from harmful content, contact and conduct, while ensuring that teaching and learning are not unreasonably restricted.

The school's filtering and monitoring arrangements form part of its wider safeguarding responsibilities and are reviewed regularly to ensure compliance with national standards.

Filtering

The school uses filtering systems designed to:

- Prevent access to illegal, harmful or inappropriate content, including extremist material, pornography, self-harm content, hate material, gambling, and known malicious sites.
- Block websites that present risks relating to misinformation, disinformation, conspiracy theories or harmful online trends.
- Support the safe use of AI-enabled tools, where filtering helps mitigate risks linked to AI-generated harmful or misleading content.
- Reduce exposure to harmful search results or content encountered accidentally or deliberately.

Filtering arrangements will be configured to balance safety with access to legitimate educational resources, ensuring that "over-blocking" does not impair teaching and learning.

Monitoring

Monitoring systems are used to:

- Identify concerning online activity on school-managed devices or accounts.
- Generate alerts when pupils attempt to access harmful content or engage in risky behaviour.
- Allow staff to intervene early where safeguarding concerns may arise.
- Support the DSL in identifying patterns, trends or repeated concerns across individuals or groups.

Monitoring may be technical (software-based), manual (supervision of devices), or both, depending on context.



CHILTON CoFE VA FOLIAT PRIMARY SCHOOL

Monitoring systems do not replace the need for supervision, education and strong safeguarding culture; they complement it.

Chilton Foliat Primary School complies with the DfE Risk Protection Arrangement (RPA) conditions in four areas:

- a) The school has offline backups via The Cloud
- b) It ensures that all employees or governors who have access to the school's information technology system undertake annual NCSC Cyber Security Training
- c) Is registered with Police Cyber Alarm
- d) Has a Cyber Response Plan in place.

The two systems used to provide filtering and monitoring support are:

- a) Securus eSafety Monitoring 360. The Headteacher has an email account via which they can receive notifications.
- b) RM Safety Net. The same.

There are established and effective routes for users to report inappropriate content, recognising that no system can be 100% effective. There is also a clear process in place to deal with, and log, requests/approvals for filtering changes. Filtering logs are regularly reviewed and alert the Designated Safeguarding Lead to breaches which are then acted upon.

Roles and Responsibilities

Headteacher

The Headteacher is responsible for ensuring:

- The school has appropriate, effective filtering and monitoring systems in place.
- Arrangements are reviewed at least annually, including through the DfE self-assessment tool.
- Decisions about what is blocked or allowed are documented and reviewed.
- Any changes to filtering settings are approved following safeguarding and curriculum considerations.

Designated Safeguarding Lead (DSL)

The DSL will:



CHILTON CofE VA FOLIAT PRIMARY SCHOOL

- Review filtering and monitoring reports regularly, responding to alerts in accordance with safeguarding procedures.
- Liaise with the IT provider to resolve concerns, adjust filtering categories and improve provision.
- Use monitoring insights to support early intervention, pastoral care and risk assessment.
- Report to governors on patterns, concerns and system effectiveness.

IT Provider

The IT provider will:

- Maintain secure, reliable and compliant systems.
- Ensure filtering and monitoring systems are up to date and working effectively.
- Inform the DSL and Headteacher of any technical concerns, vulnerabilities or notable alerts.
- Support the school to meet DfE Digital & Technology Standards.

Review and Evaluation

Filtering and monitoring systems are reviewed:

- Annually (as a minimum) using the DfE self-assessment tool.
- After significant safeguarding incidents.
- When new technologies, devices or platforms are introduced.
- When there are changes to national standards or guidance.

The school will update systems promptly in response to emerging risks, including those linked to manipulative content, deepfakes or harmful online trends.

Responding to Filtering and Monitoring Alerts

When monitoring systems generate a safeguarding alert:

- The DSL will review the alert promptly.
- Appropriate actions will be taken, which may include speaking with the pupil, contacting parents/carers, offering support or escalating to statutory agencies.
- The incident will be recorded in the Online Safety Incident Log (Appendix 6).
- Technical adjustments may be made to filtering rules if required.

Any attempt by a pupil, staff member or visitor to bypass filtering or monitoring systems is considered a serious breach of this policy and will be dealt with according to the school's Behaviour, Safeguarding and/or Staff Conduct procedures.



Social Media

Social media can offer positive opportunities for communication, collaboration and celebration of learning, but it also presents significant safeguarding, reputation and wellbeing risks. Chilton Foliat Primary School is committed to ensuring that all members of the school community use social media safely, responsibly and in a way that protects pupils, staff and the wider community.

This section outlines expectations for both staff and official school social media activity.

Expectations for Staff Use of Social Media

All staff—including teachers, support staff, volunteers, supply staff, governors and contractors—must maintain high standards of professional conduct online at all times.

Staff must:

- Not make references to pupils, parents, colleagues or the school on personal social media accounts.
- Not post images or videos of pupils or school events on personal accounts under any circumstances.
- Not engage in online discussions relating to any member of the school community.
- Ensure their privacy settings on all social media platforms are set to the highest level.
- Be aware that even with privacy settings applied, content may still become public.
- Maintain professional boundaries online, including not accepting “friend” or connection requests from pupils or former pupils under 18.
- Refrain from posting or sharing material that could bring the school into disrepute.
- Seek advice from the Headteacher or DSL if they encounter concerning content involving a member of the school community.

Staff must remember that their professional identity extends beyond the school site and that online conduct may be viewed as a reflection of the school's safeguarding culture.

Official School Social Media

Any official school-run social media accounts are managed with great care and oversight.

Before establishing or using an official platform, the school will:

- Obtain approval from the Headteacher/DSL.
- Ensure that access is limited to authorised staff only.
- Ensure that account management responsibilities are clearly defined.
- Put in place processes for regular monitoring of content and engagement.
- Follow strict safeguarding and data-protection procedures when posting content relating to pupils.



CHILTON CofE VA FOLIAT PRIMARY SCHOOL

Official school accounts will:

- Model positive, safe and responsible use of social media.
- Never post or share images of pupils without appropriate parental permissions.
- Avoid sharing personal details about staff or pupils.
- Respond appropriately to messages or interactions (e.g., not engaging in disputes or sensitive discussions online).
- Promote online safety, school values, and positive communication.

Where concerns arise regarding content posted by the school, parents/carers should contact the school directly using formal channels rather than via social media.

Online Reputation and Professional Conduct

The school recognises that the behaviour of staff, pupils and parents online can have a significant impact on the reputation and safety of the community.

Therefore:

- Defamatory, aggressive or inappropriate posts relating to the school or its members will be addressed through the Complaints Procedure or, where necessary, safeguarding or disciplinary processes.
- Parents/carers are encouraged not to use personal social media to resolve issues or air concerns about the school. Instead, they should contact the school directly so matters can be resolved appropriately.
- Pupils will be taught how to manage their online reputation and the long-term impact of posts, images and comments.

Use of Social Media for Teaching and Learning

Where social media platforms or online collaborative tools are used for educational purposes:

- Their use must be approved by the Headteacher/DSL.
- Pupils must use them only within the boundaries of supervised learning activities.
- Staff must ensure privacy settings are appropriate and no personal accounts are used.

Emerging technologies, including AI-enabled communication tools, will be assessed for risk before use in school.



Responding to Social Media Concerns

Concerns relating to social media use—for example cyber-bullying, harmful challenges, viral trends, the sharing of images, or concerning posts—must be reported to the DSL immediately.

The school will:

- Investigate concerns in line with safeguarding and behaviour policies.
- Support pupils and staff involved.
- Request content removal from platforms where necessary.
- Contact external agencies (e.g., Police, LA, Prevent) if required.

Digital and Video Images

Chilton Foliat Primary School recognises that the use of digital images and video can enhance teaching, learning, communication and celebration of pupil achievement. At the same time, the creation, storage and sharing of images present safeguarding, privacy and data-protection risks. This section sets out how images and recordings are managed safely and responsibly across the school.

General Principles

The school ensures that:

- Digital images and videos of pupils are created only for legitimate educational purposes.
- Images are used in ways that promote safety, dignity and respect for all children.
- Personal data contained within images is protected in accordance with data protection law.
- Parents/carers are informed about how images may be used and have clear opportunities to provide or withdraw consent.
- Staff, pupils, parents and visitors understand their responsibilities regarding photography and filming on the school site.

Staff Use of Digital Images

Staff and volunteers must:

- Use only school-owned devices (e.g., school cameras, iPads) to take photos or videos of pupils.
- Never use personal mobile phones or personal cameras to capture images of pupils.
- Ensure that images are stored securely on school systems, in line with the school's data-protection and retention policies.



CHILTON CofE VA FOLIAT PRIMARY SCHOOL

- Ensure that pupils are appropriately dressed and represented respectfully in any images or recordings.
- Avoid taking or sharing images that could be considered inappropriate or misleading.
- Delete images promptly once they are no longer required for their intended educational purpose, following the school's retention schedule.

No images or videos may be shared on personal messaging platforms or social media accounts.

Parental Consent

- The school obtains written parental/carer consent for the use of images and video of their child for specific purposes (e.g., displays, newsletters, website, social media, press).
- Consent is updated periodically and may be withdrawn at any time.
- The school maintains an up-to-date photographic permissions list which staff must follow.
- Pupils whose parents/carers decline consent will not be photographed or filmed in ways that make them identifiable.

Use of Images in School Publications and Online

When publishing images (e.g., newsletters, displays, website, social media), the school will ensure:

- Only images for which consent has been obtained are used.
- Pupils' full names are not used alongside images in public-facing materials, unless exceptional permission is obtained.
- Images do not reveal personal information (e.g., addresses, contact details).
- Only photographs that present pupils positively and safely are published.
- Group photographs are used wherever possible to reduce individual identification.

Use of Digital Images by Parents and Carers

Parents/carers are welcome to take photos or video of their own children at school events for personal use only. However, they must:

- Not share images or videos of other children online, including on social media.
- Respect any request from the school to refrain from photography at specific events where safeguarding considerations apply.
- Not use school events as opportunities for live-streaming or public posting.

The school reserves the right to restrict photography at events where there are safeguarding or privacy concerns.



Use of Images by External Agencies

External organisations (e.g., press, sports coaches, visiting professionals) may only take images or recordings of pupils if:

- They have obtained explicit written consent from the school.
- Parents/carers are informed when necessary.
- Images will be used in accordance with safeguarding expectations and privacy regulations.

Live-Streaming and Remote Learning

If live-streaming or video conferencing is used:

- Sessions must follow school safeguarding procedures.
- Only school-approved platforms may be used.
- Pupils must remain appropriately dressed and behave safely online.
- Staff must ensure no unauthorised recording takes place during sessions.

Responding to Concerns

If anyone becomes concerned about an image or video of a pupil:

- They must report it immediately to the DSL or Headteacher.
- Staff must not delete, forward or copy any concerning images; safeguarding procedures will be followed.
- Illegal images or content will be managed in line with statutory guidance and may be referred to the police.

Training for All Staff

All staff will receive:

- Annual safeguarding and online safety training, which includes the latest expectations from national guidance and reflects local priorities and emerging issues.
- Training on:
 - Recognising online harms, including cyber-bullying, grooming, online coercion and harmful content.
 - Risks linked to misinformation, disinformation and conspiracy theories, and how these may affect children's views, wellbeing or safety.
 - AI-related risks, such as deepfakes, digital manipulation and harmful AI-generated content.
 - Recognising indicators of online sexual harassment, online harmful sexual behaviour and peer-on-peer abuse.



CHILTON CofE VA FOLIAT PRIMARY SCHOOL

- Responding to pupils' concerns and knowing how to escalate issues safely and appropriately.
- Understanding links between attendance and online safety concerns (e.g., online exploitation, night-time gaming, coercion or harmful online relationships).

Staff training is regularly refreshed throughout the year through staff briefings, updates, professional development materials and relevant external guidance.

Designated Safeguarding Lead (DSL) and Deputy DSL Training

The DSL and DDSLs receive:

- Specialist safeguarding training at least every two years, including enhanced online safety components.
- Regular updates (at least annually) on:
 - Emerging digital harms
 - Online behavioural trends
 - AI-related risks and digital manipulation
 - Filtering and monitoring systems
 - Cyber-security expectations
 - National developments in safeguarding policy and practice

DSL training includes understanding how filtering and monitoring systems work, how to interpret alerts, and how to respond to incidents safely and proportionately.

Governors' Training

Governors will:

- Receive safeguarding and online safety training appropriate to their strategic role.
- Develop an understanding of:
 - Filtering and monitoring responsibilities
 - Oversight of cyber-security measures
 - The impact of online harms on children's wellbeing, safety and attendance
 - How school leaders manage online safeguarding risks

This ensures governors can provide informed challenge and scrutiny of the school's arrangements.

Training for Volunteers and External Visitors

Volunteers and regular visitors:



CHILTON CofE VA FOLIAT PRIMARY SCHOOL

- Will receive appropriate training or guidance based on their level of contact with pupils.
- Must read and understand key safeguarding documents, including the Acceptable Use Policy.

Ensuring Training is Embedded in Practice

The school will:

- Keep records of staff safeguarding and online safety training.
- Review training needs regularly based on incident analysis, filtering alerts and staff feedback.
- Provide targeted training where specific needs or risks are identified (e.g., gaming harm, AI misuse, harmful trends).
- Ensure that training remains current, relevant and responsive to technological and behavioural changes.

Links to other policies

This Online Safety Policy should be read alongside a range of other school policies and guidance documents that support safeguarding, behaviour, data protection and the safe use of technology. Together, these policies create a coherent and comprehensive approach to keeping pupils safe both online and offline.

The following policies are closely linked to online safety and must be considered together with this document:

- **Safeguarding and Child Protection Policy**
Sets out the school's overarching safeguarding procedures, including the management of online harms, digital safeguarding concerns and peer-on-peer abuse.
- **Behaviour Policy**
Outlines expectations for pupil conduct, including online behaviour, cyber-bullying, misuse of technology and consequences for inappropriate actions.
- **Anti-Bullying Policy**
Provides information on the prevention, identification and response to all forms of bullying, including cyber-bullying.
- **Staff Behaviour Policy / Staff Code of Conduct**
Defines expected professional conduct, including safe and appropriate online behaviour, social media use, communication, confidentiality and use of digital devices.
- **Data Protection and Privacy Notices**
Explain how the school collects, uses, stores and shares personal data, including digital images, videos, online accounts and monitoring information.



CHILTON CoFE VA FOLIAT PRIMARY SCHOOL

- **Acceptable Use Agreements (Appendices 1–4)**
Set out expectations for the use of technology by pupils, staff, volunteers, governors and visitors.
- **RSHE (Relationships, Sex and Health Education) Policy**
Includes curriculum expectations related to online relationships, digital resilience, consent, online reputation and managing online content.
- **Cyber Security and Digital Technology Standards (School ICT Policy)**
Provides details on cyber-security arrangements, device management, backups, patching and compliance with DfE digital standards.
- **Complaints Procedure**
Clarifies how parents or carers can raise concerns about online safety incidents, digital communication or school use of images or online platforms.
- **Remote Learning / Online Learning Policy** (if applicable)
Sets expectations for safe online learning, live-streaming, digital communication and remote safeguarding procedures.

This integrated approach ensures that safeguarding, online safety and digital wellbeing are embedded across the school's work and that consistent expectations apply to all members of the Chilton Foliat Primary School community.



Appendix 1: EYFS and KS1 Acceptable Use Agreement

For Pupils and Parents/Carers

Acceptable Use of the School's ICT Systems and Internet

Name of pupil: _____

When I use the school's computers, iPads, Chrome Books and the internet in school, I will:

- Ask a teacher or trusted adult before using any device.
- Only use websites or apps that a teacher or adult has said are safe.
- Tell my teacher straight away if:
 - I click on something by mistake
 - I see something that upsets me or a friend
 - Someone I don't know tries to talk to me
- Be kind and polite to others online.
- Look after the school's computers and iPads.
- Use only the username and password I have been given.
- Keep my password private.
- Never share my personal information (name, address, phone number) online.
- Save my work on the school network when asked.
- Check with a teacher before printing.
- Log off when I finish using a device.

I understand that the school will check what I do on the computer and internet. If I break the rules, I know there will be consequences.

Pupil signature: _____ Date: _____

Parent/Carer Agreement

I agree that my child can use the school's ICT systems and internet.

I will support my child to follow the rules above and to use technology safely both inside and outside school.

Parent/Carer signature: _____ Date: _____



Appendix 2: KS2 Acceptable Use Agreement

Acceptable Use of the School's ICT Systems and Internet

Name of pupil: _____

When I use school devices and the internet, I will:

- Use the school's ICT systems responsibly and for learning only.
- Only use devices when a teacher is present or has given permission.
- Keep my usernames and passwords safe and never share them.
- Keep my personal information private at all times.
- Tell a teacher immediately if I see anything that worries, upsets or confuses me.
- Always log off when I finish working.

I will not:

- Access inappropriate websites (including social media, chat rooms or gaming sites) unless allowed by a teacher for learning.
- Use rude, unkind or offensive language online.
- Open attachments or click links without checking with a teacher.
- Create, share or post inappropriate images, messages or content.
- Log in using someone else's details.
- Arrange to meet anyone I have only spoken to online.

I understand that the school checks the websites I visit and that I must follow these rules.

Pupil signature: _____ Date: _____

Parent/Carer Agreement

I agree that my child can use the school's ICT systems and internet.

I will support my child to follow the rules above and to use technology safely both inside and outside school.

Parent/Carer signature: _____ Date: _____



Appendix 3: Acceptable Use Agreement — Staff, Governors, Volunteers and Visitors

Acceptable Use of the School's ICT Systems and Internet

Name: _____

When using the school's ICT systems or accessing the internet (on-site or on a work device), I will:

I will not:

- Access or attempt to access inappropriate material, including content that is illegal, violent, abusive, extremist, discriminatory or pornographic.
- Create, send, share or link to inappropriate content.
- Use personal social media to discuss or reference pupils, parents, colleagues or the school.
- Install unauthorised software or connect unauthorised devices.
- Share my password with anyone or allow others to use my login.
- Take photographs of pupils on a personal device.
- Share confidential information or personal data unlawfully.

I will:

- Use ICT systems only for professional, educational or authorised purposes.
- Keep devices secure, password-protected and updated.
- Follow data-protection legislation and school policies at all times.
- Report any online safety concerns, misuse or breaches immediately to the DSL/Headteacher.
- Model safe, respectful and responsible online behaviour.

Signature: _____ **Date:** _____



Appendix 4: Staff Laptop & iPad Acceptable Use Policy

Name of staff member: _____

School devices are provided to support professional duties. When using school laptops or iPads, I agree to:

Keeping the device secure

- Keep the device password-protected.
- Enable automatic locking and never share access.
- Avoid using the device on unsafe public Wi-Fi.
- Store the device securely at home and school.
- Understand that insurance does not cover theft from an unattended vehicle.

Safe use

- Use the device only for work purposes.
- Ensure all data—especially pupil information—remains protected and encrypted.
- Use only school-approved systems for storing pupil data.
- Not allow family members to use the device.
- Not share or post photos of pupils on personal accounts.

If issues arise

- Report loss, damage, theft or suspicious activity immediately.
- Cooperate with safeguarding or cyber-security checks on the device.

Signature: _____ Date: _____



Appendix 5: Online Safety training needs – self-audit for staff

ONLINE SAFETY TRAINING NEEDS AUDIT

Name of staff member/volunteer:	Date:
Question	Yes/No (add comments if necessary)
Do you know the name of the person who has lead responsibility for online safety in school?	
Are you aware of the ways pupils can abuse their peers online?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	



CHILTON CoFE VA FOLIAT PRIMARY SCHOOL

Appendix 6: Online Safety Incident Report Log

ONLINE SAFETY INCIDENT LOG				
Date	Where the incident took place	Description of the incident	Action taken	Name and signature of staff member recording the incident