



Christleton Primary School
Be the best you can be

E-Safety Policy

Document Name		Reviewed by	
E-Safety Policy		Full Governing Body	
Author	Mr Mitchell/Mrs Shaw	Version number	2.0
Date of Policy	Policy Reviewed	Next Review	
September 2026		September 2027	
Signed Headteacher			
Signed Chair of Governors			

1. Purpose and principles

Online safety is part of safeguarding and applies to all use of digital technology, whether on school systems, personal devices, at home, during remote learning or outside school where harm affects pupils or the school community. Christleton Primary School aims to help pupils become safe, respectful, critical and confident users while maintaining appropriate technical protection and a clear response to harm.

The school will balance safety with access to a broad curriculum. Filtering will not be so restrictive that it unreasonably limits learning or disproportionately affects pupils with SEND or protected characteristics; neither will educational value be used to justify avoidable exposure to harm.

2. Legal and guidance framework

This policy has regard to KCSIE 2026, the DfE filtering and monitoring and cyber-security standards, teaching online safety in schools, the Prevent duty, the Equality Act, data-protection law, the Computer Misuse Act, statutory Relationships Education/Health Education and Computing requirements, and current guidance on sharing nudes and semi-nudes, cyberbullying, searching and confiscation.

3. Online risk

The school considers four overlapping areas of risk:

- Content - exposure to illegal, harmful, misleading or age-inappropriate material, including pornography, violence, hate, self-harm, suicide, eating-disorder content, misinformation, extremist material and harmful generative-AI output.
- Contact - harmful interaction with adults or peers, including grooming, coercion, exploitation, bullying, sexual harassment, impersonation, scams and pressure to share images or information.
- Conduct - a pupil's own behaviour, including oversharing, bullying, sexual-image sharing, copyright infringement, unsafe challenges, livestreaming, cheating, creating harmful content and revealing location.
- Commerce - gambling-like features, in-app purchasing, advertising, financial scams, phishing, identity theft, data exploitation and inappropriate contractual or age-restricted services.

4. Roles and governance

4.1 Governing board

- Ensure appropriate filtering and monitoring systems are in place, regularly reviewed and informed by the school's risk profile.
- Receive at least annual assurance on effectiveness, incidents, training, curriculum and compliance without accessing unnecessary pupil-level data.
- Ensure online safety is included in safeguarding training and that governors understand the expectations they oversee.

4.2 Headteacher

- Provide resources, designate competent leads, enforce staff conduct requirements and ensure the policy works across curriculum, safeguarding, IT, data protection and behaviour.

4.3 DSL

- Lead safeguarding response to online concerns; ensure monitoring alerts are triaged; assess child-on-child abuse, exploitation, Prevent and external-referral needs; and maintain appropriate records.

4.4 Online safety and computing lead

- Coordinate curriculum progression, staff/parent guidance and policy evaluation. The lead is Julie Shaw.

4.5 Technical/filtering and monitoring lead

- Maintain systems, access controls, logs, testing and supplier assurance. Strategic responsibility remains with school leaders and governors and is not outsourced. The technical lead/provider is Dan Woolley.

4.6 Staff, pupils and parents

- Staff model safe practice, supervise proportionately, use school-approved systems and report concerns immediately.
- Pupils follow age-appropriate acceptable-use expectations, protect passwords, treat others respectfully and report worrying content/contact without fear of automatic blame.
- Parents support safe routines, age restrictions and reporting and tell the school where online harm affects education or safety.

5. Filtering and monitoring

The school will identify and assign roles; review filtering and monitoring effectiveness at least once each academic year; check that filtering and monitoring work as intended; review reports and incidents; and adapt provision to pupil age, SEND, EAL, safeguarding profile, devices and curriculum needs.

The annual review will record systems used, responsible people, categories blocked/allowed, monitoring arrangements, test results, risks, over/under-blocking, remote/BYOD coverage, staff access, supplier assurance and actions. Governors will receive a summary and challenge unresolved risks.

Regular checks will be carried out at termly or following any incident. Attempts to access blocked content, monitoring alerts and technical weaknesses will be recorded and triaged. A technical alert is not automatically proof of misconduct; context and safeguarding need must be considered.

Temporary unblocking for legitimate learning requires authorised, time-limited and logged approval. Staff must not bypass controls through personal hotspots, VPNs or unapproved accounts.

6. Accounts, passwords and access

- Users will have individual accounts where appropriate and will not share passwords. Multi-factor authentication will be used where the DfE cyber standard requires or recommends it.
- Access will follow least-privilege principles and be removed promptly when a user leaves or changes role.
- Administrative accounts will not be used for routine activity. Software, browser extensions, apps and cloud services require approval.
- Suspected compromise must be reported immediately; users should not continue experimenting with or investigating an attack themselves.

7. Curriculum and education

Online safety will be taught progressively through Computing, Relationships and Health Education, PSHE, English and across the curriculum. Teaching will be age and development appropriate and revisited in response to emerging risks.

- Pupils learn how to evaluate accuracy, bias, advertising, persuasion and synthetic or AI-generated content.
- Pupils learn privacy, consent, passwords, digital footprint, copyright, scams and safe reporting.
- Pupils learn what healthy and respectful online relationships look like and that pressure, secrecy, threats or requests for sexual images are warning signs.
- Pupils learn how algorithms, recommendation systems and persuasive design may affect attention and choices.
- Pupils are taught not to blame a child who has been tricked, exploited or shared something under pressure, and how to seek help.

Before introducing a website, app or platform, staff will evaluate educational purpose, age terms, privacy, advertising, data processing, accessibility, safeguarding controls and whether parental information/consent is required. Approval will be recorded through the school's external IT support.

Online Communication and eSafety	Introduction Ask children to write down or draw pictures of the sites they visit, apps or games they play on. Discuss with the children what things they do online and use their information to help plan the e-safety lessons this year.	Commonsense Media Staying Safe Online The internet allows pupils to experience and visit places they might not be able to see in person. But, just like travelling in the real world, it's important to be safe when travelling online. On this virtual field trip, pupils can practice staying safe on online adventures. DL1.5 EICW • Privacy and Security • Managing online information	Sharing Images Do the children know of any places on the internet where they could put their picture? Tell the pupils their pictures on a tablet should not be shared with other people you don't know. Support using Jessie and Friends: Sharing Pictures Film DL1.5 EICW • Copyright and Ownership • Managing online information • Privacy and Security	Smartie the Penguin Use Y1 resources from Childnet to look at what we share on the internet. Join in with Mummy Penguin's song and follow the adventures of Smartie the Penguin as he learns how to be safe on the internet. The first version of story covers the following 3 themes: • Pop ups and in app purchasing • Inappropriate websites for older children • Cyberbullying Download teacher resources and lesson plans for Year 1. DL1.5 EICW • Online Bullying • Privacy and Security • Online Reputation	Common Sense Materials Media Balance Use the Common Sense Media lesson to explore how pupils need to consider the feelings of themselves and others when making decisions about when, where, and how much to use technology. DL1.5 EICW • Managing online information • Self-image and identity • Online Bullying • Health, well-being and lifestyle	Common Sense Materials Pause for thought Often, pupils find it hard to transition from an online activity to an offline one. Teach pupils a simple routine for how to manage those inevitable digital interruptions that are part of life in the digital age. DL1.5 EICW • Health, well-being and lifestyle • Self-image and identity • Health, well-being and lifestyle
--	---	--	--	--	--	---

8. Supervision and classroom practice

Supervision will reflect age, activity and risk. Screens will be visible where practicable, search tasks will be structured and pupils will use approved accounts. Staff will not instruct pupils to falsify age or create personal accounts for school work.

Accidental access to inappropriate content will be reported without automatic sanction. Staff will close/minimise exposure, reassure pupils, record the URL/context, notify the technical lead/DSL as appropriate and avoid repeatedly viewing the content.

9. Personal devices, mobile phones and wearable technology

Pupil mobile phones and personal connected devices are governed by the Behaviour Policy and school rules. Trackers, cameras and smartwatches must not undermine privacy, safeguarding or assessment.

Staff personal devices will not be used to photograph, record or communicate with pupils except under an expressly approved school procedure. School information will not be stored in unapproved personal apps or accounts.

10. Images, video, livestreaming and remote learning

School images and recordings will be created, stored and published only for an identified purpose and under the school's privacy/consent arrangements. Livestreaming requires risk assessment, controlled access, appropriate backgrounds, waiting rooms/permissions where relevant and no recording unless authorised.

Remote contact will use approved school accounts, professional hours and auditable channels. One-to-one contact will be visible or otherwise safeguarded according to context. Staff will not use personal social-media accounts or personal messaging numbers to communicate with pupils.

11. Social media and online reputation

Staff must maintain professional boundaries and confidentiality online and follow the Staff Code of Conduct. They must not discuss pupils, families, colleagues or confidential school matters on personal accounts. Pupils and parents are encouraged to raise concerns through school channels rather than identify children or staff publicly.

The school may respond to online behaviour outside school where it creates safeguarding risk, bullying, harassment, reputational or operational harm within the headteacher's lawful authority.

12. Generative artificial intelligence

AI tools may be used only where approved, age appropriate and educationally justified. Users must not enter personal, safeguarding, confidential, copyrighted or assessment-sensitive information into an unapproved tool. AI output must be checked for accuracy, bias, inappropriate content and fabricated sources.

Pupils will be taught when AI assistance is permitted and how to acknowledge it. Staff remain professionally responsible for teaching, assessment, communication and decisions and must not rely on AI to make safeguarding, SEND, behaviour or employment decisions.

13. Responding to online safety incidents

1. Protect the child and address any immediate danger. Do not promise confidentiality.
2. Report safeguarding concerns to the DSL immediately; use 999 where there is immediate risk.
3. Preserve relevant evidence without circulating it. Record account names, URLs, dates and the child's account in their own words where appropriate.
4. Do not investigate beyond role, contact an alleged perpetrator or delete material that police/CEOP may need without advice.
5. Consider parents, police, children's social care, LADO, Prevent/Channel, CEOP, Internet Watch Foundation, DPO/ICO, NCSC/Action Fraud and platform reporting according to the issue.
6. Provide support, risk assessment, education and proportionate behaviour response; review technical and curriculum controls.

14. Sharing nudes and semi-nudes and sexual content

Any report that a child has shared, received or been pressured to create a nude or semi-nude image is a safeguarding matter and must be referred to the DSL. Staff must not view, copy, print, forward or ask a pupil to send the image. If an image is displayed unexpectedly, staff should close the device where possible and seek DSL advice.

The DSL will follow current UKCIS guidance, consider age, coercion, exploitation, adult involvement, onward sharing and immediate risk, and decide parent/police/social-care referrals. A child will be supported and not automatically criminalised or punished for seeking help.

15. Searching devices and confiscation

Any search or confiscation of a pupil device will comply with the Behaviour Policy and DfE Searching, screening and confiscation guidance. Authorised staff may examine data or delete files only where lawful and appropriate. Where material may be evidence of a crime or safeguarding concern, staff will consult the DSL and police before deletion.

16. Cyber security and data breaches

The school will maintain patching, backups, malware protection, access control, recovery testing and supplier arrangements in line with DfE standards. A cyber incident will be reported immediately to the headteacher/IT lead, affected systems isolated where advised and evidence preserved. The business-continuity and critical-incident plans will be activated where needed.

The DPO will assess personal-data breaches and notify the ICO and affected people where legally required. Ransom demands or attacker contact will not be handled without specialist/local-authority and law-enforcement advice.

17. Training, parent partnership and review

All staff receive online-safety and filtering/monitoring training at induction and regular updates. DSLs, governors, technical staff and curriculum leads receive role-specific development. Pupils and parents receive timely guidance about emerging risks and reporting routes.

The policy and online-safety risk assessment will be reviewed annually and after significant incidents or technology changes. The governing board will receive the annual filtering and monitoring review and confirmation that actions have been completed.

Appendix 1

(Please refer to Cheshire West and Chester's Acceptable Use Policy)

Appendix 2

Acceptable use policies (AUP's)

- Staff
- KS2
- KS1

Key Stage 2 – All children to discuss this with class teacher and when they understand, sign next to the agreement which will be displayed in class.

Safe Computing!

- ☒ I understand what I need to do to **protect my personal safety** online.
- ☒ I **care for the equipment** correctly including storage, not changing the settings, using what I am allowed to and informing an adult if something is damaged.
- ☒ I **stay safe online** and treat others as I would expect to be treated. I will not share images or copy others work without permission and will always be polite and respectful.
- ☒ I **will not use my personal devices in school.**
- ☒ I **do not use social media platforms unless instructed** to do so.
- ☒ I **am responsible when using technology** in and out of school.
- ☒ **Tell an adult** if I see something that upsets me on the screen.
- ☒ I have read the schools **Acceptable use Agreement** and have agreed to follow it.



Key Stage 1 – The children will discuss this with the class teacher and the details will be explained so that they understand this agreement. No signatures are required in KS1.

Safe Computing!

☒ **Ask before I use** either a computer or iPad.

☒ **Stick to the app or software** my teacher has asked me to use.



☒ Take **care** of the equipment.

☒ **Ask for help** if I am unsure or have done something wrong.

☒ **Tell an adult** if I see something that upsets me on the screen.

