

Online Safety Policy

This policy document should be read in conjunction with the safeguarding policy, teaching and learning policy, anti-bullying policy, computing policy and remote learning policy to ensure that online safety is embedded properly across the school.

This policy document is drawn up to protect all parties – the pupils, the staff and the school and aims to provide clear advice and guidance on how to minimise risks and how to deal with any infringements.

If a member of staff or a school visitor has a concern regarding Online safety, they must speak to a member of the safeguarding team without delay and log the incident on CPOMS.

Aims

Online safety has become an essential part of daily life for children. Our learners are using technology from a very young age so it is vital they learn how to stay safe. At school, we provide children with a robust, spiral curriculum that unpicks what it means to be a safe and responsible user online. We allow children the opportunity to discuss how the online space can be both a positive, and occasionally challenging, experience. By providing children with a safe and controlled environment in school, we aim for them to be able to take those skills outside of the school gates to use at home.

The philosophy of 'empowering children to stay safe' includes aims that children are:

- safe from maltreatment, neglect, violence and sexual exploitation;
- safe from accidental injury and death;
- safe from bullying and discrimination;
- safe from crime and anti-social behaviour in and out of school;
- secure, stable and cared for.
- have the understanding of misinformation, disinformation and conspiracy theories.

These uphold articles 16 and 19 of the UNCRC.

Chesterton Primary School aims to:

- protect and educate pupils and staff in their use of technology;
- have the appropriate mechanisms to intervene and support any incident where appropriate.

Online safety encompasses the use of new technologies, internet and electronic communications such as mobile phones, social media and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

As stated in the 2025 guidance for 'Keeping Children Safe in Education', the breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk:

Content: being exposed to illegal, inappropriate, or harmful content, for example: pornography, racism, misogyny, self-harm, suicide, antisemitism, radicalisation, extremism, misinformation, disinformation (including fake news) and conspiracy theories.

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

Conduct: online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying; and

Commerce - risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group (<https://apwg.org/>).

Keeping children safe in education 2025

The Risks

Much of these aims apply equally to the 'virtual world' that children and young people will encounter whenever they use ICT in its various forms. For example, we know that the internet has been used for grooming children and young people with the ultimate aim of exploiting them sexually; we know that ICT can offer new weapons for bullies, who may torment their victims via websites or text messages; and we know that children and young people have been exposed to inappropriate content when online, which can sometimes lead to their involvement in crime and anti-social behaviour. Exposure to misinformation, disinformation and conspiracy theories is increasing with the presence of social media. It is the duty of the school to ensure that every child in their care is safe, and the same principles should apply to the 'virtual' or digital world as would be applied to the school's physical buildings.

The Internet is an open communications channel, available to all. Anyone can send messages, discuss ideas and publish material with little restriction. These features of the Internet make it both an invaluable resource used by millions of people every day as well as a potential risk to young and vulnerable people. Much of the material on the Internet is published for an adult audience and some is unsuitable for pupils. At Chesterton, we are committed to providing pupils with as safe an Internet environment as possible and to teach pupils to be aware of and respond responsibly to any risk.

Overview

Creating a safe ICT learning environment includes three main elements at this school:

- An effective range of technological tools (including forensic software);
- Policies and procedures, with clear roles and responsibilities;
- An online safety education programme for pupils, staff and parents.

Handling online safety complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the Headteacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures (see appendix D)

Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018. (See data protection policy)

Internet access

- Access to the Internet will be under adult supervision to ensure pupils access specific, approved on-line materials.
- Pupils, parents and staff will be asked to sign a consent form as part of the enrolment process (for staff see data protection policy)
- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

School network safety measures

The school maintains broadband connectivity through the LGfL. Additionally, the school has up-to-date antivirus, anti-spyware and anti-spamware software and approved firewall solutions installed on their network. To make sure rogue applications are not downloaded and hackers cannot gain access to the school's equipment or into users' files through Internet use, staff and pupils are not able to download executable files and software. Unfortunately, there is the potential for inappropriate material to get through any filtering system. Any inappropriate site will be reported to the Designated Member of staff for Safeguarding and access to inappropriate sites will be blocked.

Social Networking

- Pupils will be advised never to give out personal details of any kind which may identify them or their location.
- Pupils will learn about sensible use and how to make their profiles private.
- Pupils will also learn about the report features to be used on social networking sites if they have any problems.
- We filter access to social networking sites unless a specific use is approved.
- Pupils will be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications.

E-mail

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal personal details of themselves or others.
- All staff must use the Chesterton approved staff e-mail for all school related e-mails.

School Website

- The contact details on the website should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.
- It is the policy of the school to not allow pupils surnames or for any photographs which clearly identify any pupil to be used on the school website without the parents/carers permission.
- Content on the school website must not infringe copyright or intellectual property rights through any content published on the website.

- Links to any external websites should be thoroughly checked before inclusion on a school website to ensure that the content is appropriate both to the school and for the intended audience.

Mobile phones

Pupils:

- Mobile phones are not allowed to be used during the school day.
- They must be handed into the office at the beginning of the school day and collected at the end of school day.
- Mobile phones should not be taken on school trips including residential.

Staff:

- Cameras on phones cannot be used to take or store photos of children.
- Mobile phone calls are not allowed to be answered during lesson times, and they should be made in the staff room or outside of the school perimeter.
- Mobile phones are allowed on school trips.
- Mobile phones should have a passcode enabled to prevent any personal information being obtained by pupils.

Cyber Bullying

Cyber bullying is when a person or a group of people uses the internet, mobile phones, online games or any other kind of digital technology to threaten, tease, upset or humiliate someone else. The school will help prepare pupils for the hazards of using technology while promoting learning and social opportunities. Cyber bullying is a form of bullying but because it happens online or on mobile phones it can happen 24 hours a day, seven days a week. Any issues of Cyber Bullying will be dealt with in line with the Anti-Bullying Policy.

Child on child Abuse

Child on child abuse can manifest itself in many ways and can include, but is not limited to, bullying (including prejudice based and discriminatory) cyberbullying, sexting, gender-based violence, sexual abuse, up skirting and hazing/initiation abuse. All staff should recognise that children are capable of abusing other children (including online). It often manifests itself through the use of mobile devices and the internet. Child on child abuse is not tolerated at Chesterton Primary School and it should not be passed off as “banter” or “part of growing up”. In the case of child on child abuse, our Safeguarding Policy and Anti-Bullying Policy should be invoked. Our Safeguarding Policy and this Online safety Policy set out the procedures taken by the school to minimise the risk of peer on peer abuse, and the Safeguarding Policy clearly states how allegations of child on child abuse will be investigated and dealt with.

Prevent

In line with our commitment to minimise the risk of pupils being radicalised, pupils’ use of school computers is monitored and pupils found searching websites or using criteria that would suggest an interest in terrorism/radicalisation are immediately reported to the safeguarding team via a cause for concern form. The matter will then follow the procedures set out in the safeguarding policy.

Sexting/Youth Produced Sexual Imagery

Sexting is when someone shares sexual, naked or semi-naked images of themselves or others, or sends sexually explicit messages. They can be sent on any device that allows you to share media and messages. Sexting can be seen as harmless by young people but creating or sharing explicit images of a child is illegal, even if the person doing it is a child. A young person is breaking the law if they:

- Take an explicit photo or video of themselves or a friend
- Share an explicit image/video of a child, even if it is shared between those of the same age
- Possess, download or store an explicit photo/image or video of a child, even if the child gave their permission for it to be created

In the most recent guidance produced by the UK Council for Child Internet Safety, Sexting in Schools and Colleges Resource Pack, sexting is referred to as “youth produced sexual imagery”, although KCSIE (September 2024) still refers to “sexting”.

Incidents of “sexting” will be investigated and dealt with in line with the safeguarding policy.

Teaching of Online safety

Governing bodies and proprietors should ensure online safety is a running and interrelated theme whilst devising and implementing their whole school or college approach to safeguarding and related policies and procedures. This will include considering how online safety is reflected as required in all relevant policies and considering online safety whilst planning the curriculum, any teacher training, the role and responsibilities of the designated safeguarding lead (and deputies) and any parental engagement.

Keeping Children Safe in Education (September 2025)

- Pupils will be informed that network and internet use will be monitored.
- Pupils will be reminded about safe use of ICT every term and each half term will have a specific online safety focus (see curriculum map for objectives each half term)
- Pupils will learn about online safety in computing lessons and PSHCE lessons. It will also be embedded in cross-curricular lessons. Additional lessons are provided when needed.
- Pupils are taught about our ‘No Blame’ culture so pupils feel able to report any bullying, abuse or inappropriate materials immediately.
- There will be an assembly each term which will raise awareness of online safety and focus on developing pupil understanding.
- Parents will be offered workshops around online safety at least once a year.

School staff

All staff are responsible for promoting and supporting safe behaviours in classrooms and the wider school by following school online safety procedures. Central to this is fostering a ‘No Blame’ culture so pupils feel able to report any bullying, abuse or inappropriate materials. All staff should be familiar with the schools’ Online safety Policy and have to sign the Acceptable Use Policy (see data protection policy).

Monitoring, Evaluation and Review

The school will review this policy annually and assess its implementation and effectiveness. The policy will be promoted and implemented throughout the school.

Policy Sign off – Online Safety Policy

	Reviewer	Date	Approver	Date
Reviewer / approver	C.Mogan	October 2025	LAC	07/10/25
	Next Review			September 2026



Appendix D

Consequences for inappropriate use of school owned technology or use of technology on the school site

Category A

- Use of non-educational sites during lessons
- Unauthorised use of email
- Unauthorised use of mobile phone (or other new technologies) in lessons
- Use of unauthorised instant messaging / social networking sites
- Accidentally corrupting or destroying others people's data (e.g. deleting online books reviews/computer work etc)
- Accidentally accessing offensive material but informs a member of staff.

Action to take: Class teacher to deal with and inform the parent of child involved.

Category B

- Continued use of non-educational sites during lessons after being warned
- Continued unauthorised use of email after being warned
- Continued unauthorised use of mobile phone (or other new technologies) after being warned
- Continued use of unauthorised instant messaging / social networking sites
- Use of Filesharing software e.g. Napster, Vanbasco, BitTorrent, LiveWire, etc
- Accidentally corrupting or destroying others' data without notifying a member of staff of it (e.g. deleting online books reviews/computer work etc)
- Accidentally accessing offensive material and not logging off or notifying a member of staff of it

Action to take: Phase leader to deal with and inform the parent of child involved.

Category C

- Deliberately corrupting or destroying someone's data (online books reviews/computer work etc)
- Deliberately violating privacy of others (e.g hacking into their account/using other people's passwords etc)

- Sending or making an email/message/social media text or video message that is regarded as harassment or of a bullying nature (one-off)
- Sending or making an email/message/social media text or video message that is regarded as offensive e.g. racist/sexist/homophobic/transphobic etc. (one-off)
- Deliberately trying to access offensive or pornographic material
- Any purchasing or ordering of items over the Internet in school time

Actions to take: Refer to SLT and online safety form to be completed. Phase leader to inform the child's parents and parents of any child involved in the incident. (Detention)

Other safeguarding actions:

If inappropriate web material is accessed:

1. Secure and preserve any evidence if possible
2. SLT to ensure appropriate technical support filters the site
3. SLT Inform ICT technician and LGfL if needed
4. Phase leader to ensure inappropriate comments/material posted by the child/children is removed.

Category D

- Continued sending or making email/message/social media texts or video messages of a bullying nature after being warned
- Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent
- Bringing the school name into disrepute (e.g. posting online videos in school uniform that are deemed inappropriate in content/ videoing and posting messaging whilst on the school grounds in school time).

Actions to take: Refer to SLT and CPOMS form to be completed. SLT to speak to the child's parents and parents of any child involved in the incident. (Detention & removal of equipment in school if needed.)

Other safeguarding actions:

1. Secure and preserve any evidence
2. SLT to ensure appropriate technical support filters the site
3. SLT Inform ICT technician and LGfL if needed