



CHALFORD HILL PRIMARY SCHOOL

Online Safety Policy

Reviewed: June 2026
Review Due: June 2027

This policy must be read in conjunction with Acceptable User Agreements for staff, volunteers and pupils.

This Online Safety Policy will be reviewed in line with the Governors' policy review timetable and with reference to any significant new developments in the use of the technologies, new threats to Online Safety or incidents that have taken place.

Appendix 1 – Useful links

Appendix 2 - Glossary of terms (Provided by Exa Networks)

Note: The following documents are published separately:

- Data Protection policy
- Pupil Acceptable Use Agreement
- Staff Acceptable Use Agreement
- Volunteer Acceptable Use Agreement

School Internet Filtering is managed by Exa Networks.

Rationale

Technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The Internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. This Online Safety policy is intended to help ensure safe and appropriate use of these technologies.

Despite the many positive aspects to these tools, there are potential risks. These fall into 4 areas of risk as identified in Keeping Children Safe in Education 2025.

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

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: personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images and online bullying

Commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams

Many of these risks reflect situations in the off-line world and this policy is to be used in conjunction with other school policies - behaviour, anti-bullying and child protection

policies. As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

We have a duty to safeguard our pupils and our aim is to do everything that could reasonably be expected of us to manage and reduce risks. The Online Safety policy that follows explains how we intend to do this.

Scope of the Policy

This policy applies to all members of the school community (including Governors, staff, pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of school.

The Education and Inspections Act 2006 empowers Head teachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other Online Safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

The 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.

Education in Online Safety: Roles and Responsibilities

The education of pupils in Online Safety is an essential part of the school's Online Safety provision and is the responsibility of all members of the school community. Children and young people need the help and support of the school to recognise and avoid online risks and build their resilience.

Online Safety education will be provided by:

- An integrated Online Safety programme through the Computing and PHSE Schemes of Work.
- The reinforcement of key safety messages through planned programme of assemblies and tutorial/pastoral activities.
- The reinforcement of key safety messages in other Computing lessons.
- To be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information.
- Pupils being helped to understand the need for the pupil AUP and encouraged to adopt safe and responsible use of ICT, the Internet and devices both within and outside school.
- Pupils being taught to acknowledge the source of information used and to respect copyright when using material accessed on the Internet.
- Staff acting as good role models in their use of ICT, the Internet and devices.

The roles described below are not exclusive to the individuals described.

Governors

Governors are responsible for reviewing the effectiveness of the policy. Governors should take part in Online Safety training/awareness sessions, with particular importance for those who have particular responsibility for safeguarding, online safety or health and safety. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority, National Governors Association, Exa Networks or other relevant organisation.
- Participation in school training/information sessions for staff or parents.
- The school's safeguarding audit will monitor the impact of the policy using:
 - Logs of reported incidents.
 - Surveys / questionnaires of pupils, parents / carers and staff.

Governors will be expected to sign the Staff/Volunteer AUP.

The Designated Safeguarding Lead (DSL)

The DSL is responsible for:

- Ensuring the safety (including Online Safety) of members of the school community, though the day-to-day responsibility for Online Safety may be delegated to suitable others.
- Ensuring that staff receive suitable CPD to enable them to carry out their Online Safety roles and to train other colleagues, as relevant.
- Ensure that all staff are aware of the procedures that need to be followed in the event of an Online Safety incident taking place.
- Support appropriate staff to liaise with the Local Authority/Exa Networks as relevant.
- Monitor the log of incidents to inform future Online Safety developments.

The DSL is to stay current in Online Safety issues and be aware of the potential for serious child protection issues to the areas of risk outlined in KCSiE 2025.

Our Designated Safeguarding Lead is: *David Poad, DSL and head teacher*

Our Computing Lead is: *Abi Stokes*

Should serious Online Safety incidents take place, the following external persons / agencies may be informed: LA Safeguarding Officer, Head Teacher, Online Safety Officer, DSL, Police.

The Head teacher and another member of the Senior Management Team will be aware of the procedures to be followed in the event of a serious Online Safety allegation being made against a member of staff.

Our Technical Advisors *Focus Networks* will:

- Put in place appropriate filtering and monitoring systems which are updated on a regular basis.
- Ensure users may only access the school's networks through properly enforced password protection
- Ensure the school's ICT infrastructure is secure and is not open to misuse or malicious attack.

- Ensure that the school's ICT systems are secure and protected against viruses and malware and that such safety mechanisms are updated regularly.
- Keep up to date with Online Safety technical information in order to effectively carry out their Online Safety role and inform and update others as relevant.
- Conduct full security checks and monitor the school's ICT systems regularly (monthly?)
- Work with SWGfL to block access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.

Online access is filtered by Exa Networks.

Teaching and Support Staff

Teaching and Support Staff are responsible for ensuring that they have an up to date awareness of Online Safety matters and of the current school Online Safety policy and practices. It is essential that all members of staff receive Online Safety training and understand their responsibilities, as outlined in this policy.

Training will be offered:

- Through staff meetings/CPD.
- As part of the induction programme for new staff.
- Through advice / guidance / training as required to individuals as required.

They should also ensure that:

- They have read, understood and signed the school Staff Acceptable Use Agreement (AUP).
- They report any suspected misuse or problems to the DSL or Computing lead for investigation.
- Digital communications with students / pupils (email / Virtual Learning Environment (VLE) / voice) should be on a professional level.
- Online Safety issues are embedded in all aspects of the curriculum and other school activities.
- Students/pupils understand and follow the school Online Safety and acceptable use policy.
- Students/pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- They monitor ICT activity in lessons, extra-curricular and extended school activities.
- They are aware of Online Safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices.
- In lessons where Internet use is pre-planned, pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in Internet searches.

The Staff AUP will be reissued every two years.

Pupils

Pupils are responsible for using the school ICT systems in accordance with the Student / Pupil Acceptable Use Policy. The Pupil AUP will be re-issued every two years.

Parents and Carers

Parents/Carers play a crucial role in ensuring that their children understand the need to use the Internet / mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will attempt to help parents understand these issues through parents' evenings, presentations, newsletters, letters, website and information about national/local Online Safety campaigns and literature. Parents and carers will be responsible for endorsing (by signature) the Pupil Acceptable Use Policy (AUP).

Communications

	Staff			Pupils			
Communication Technologies	Allowed	Allowed where appropriate*	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school in y6	☐				☐	☐	
Use of mobile phones in lessons		☐					☐
Use of mobile phones in social time	☐						☐
Taking photos with GDPR implications on personal mobile phones or other personal devices			☐				☐
Taking photos without GDPR relevance on personal mobile phones or other personal devices	☐						☐
Use of personal email addresses in school, or on school network	☐						☐
Use of school email for personal emails			☐				☐
Use of chat rooms / facilities		☐					☐
Use of social networking sites		☐					☐
Use of blogs	☐			☐			

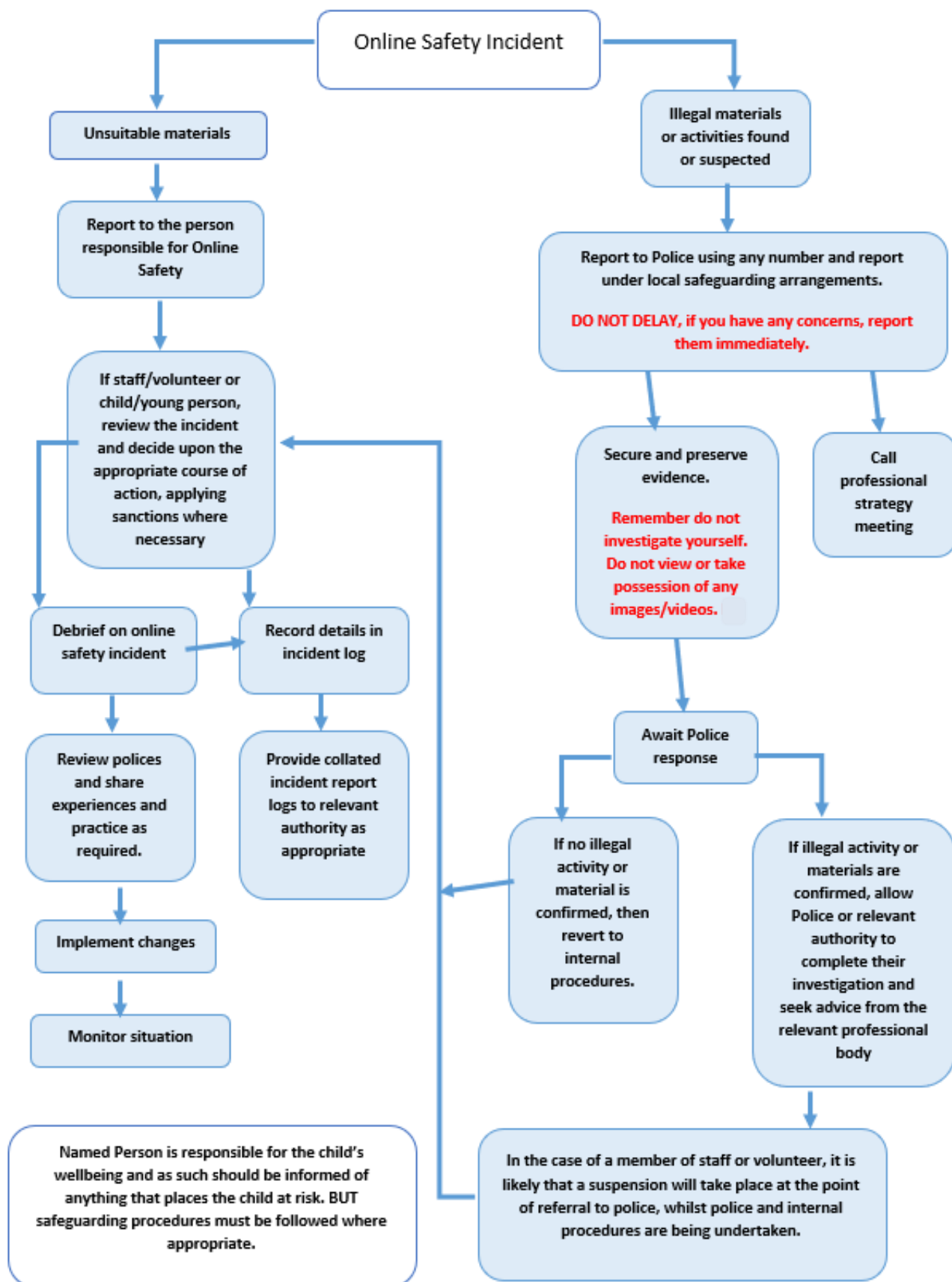
*Appropriate use would include: where there is no risk to pupils' safety, online or otherwise; where there is no conflict with the principles or policies of GDPR; where use of personal devices does not infringe good professional conduct or other school policies. If in doubt, staff should clarify with a line manager.

When using communication technologies the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems. When staff have good cause to use personal email accounts, they will treat correspondence in the manner they would treat correspondence through the school email service.
- Users are made aware that email communications may be monitored.
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff and students/pupils or parents/carers will be professional in tone and content.
- Pupils are provided with individual school email addresses for educational use.
- Students / pupils will be taught about email safety issues, such as the risks attached to the use of personal details. They will also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.

Appendix 1:

In the case of an online safety incident, the following flow chart will be used:



Appendix 2: Links to other organisations or documents

Safer Internet Centre – <https://www.saferinternet.org.uk/>

Childnet – <http://www.childnet-int.org/>

Professionals Online Safety Helpline - <http://www.saferinternet.org.uk/about/helpline>

CEOP - <http://ceop.police.uk/>

ThinkUKnow - <https://www.thinkuknow.co.uk/>

UK Council for Child Internet Safety (UKCCIS) - www.education.gov.uk/ukccis

Netsmartz - <http://www.netsmartz.org/>

360 Degree Safe – Online Safety self-review tool – <https://360safe.org.uk/>

Anti-Bullying Network – <http://www.antibullying.net/cyberbullying1.htm>

Professional Standards / Staff Training

DfE – [Keeping Children Safe in Education](#)

DfE - [Safer Working Practice for Adults who Work with Children and Young People](#)

Appendix 3: Glossary of Terms

- AUP / AUA** Acceptable Use Policy / Agreement – see templates earlier in this document
- CEOP** Child Exploitation and Online Protection Centre (part of UK Police, dedicated to protecting children from sexual abuse, providers of the Think U Know programmes.
- CPD** Continuous Professional Development
- FOSI** Family Online Safety Institute
- ICO** Information Commissioners Office
- ICT** Information and Communications Technology
- ICTMark** Quality standard for schools provided by NAACE
- INSET** In Service Education and Training
- IP address** The label that identifies each computer to other computers using the IP (internet protocol)
- ISP** Internet Service Provider
- ISPA** Internet Service Providers' Association
- IWF** Internet Watch Foundation
- LA** Local Authority
- LAN** Local Area Network
- MIS** Management Information System
- NEN** National Education Network – works with the Regional Broadband Consortia (e.g. SWGfL) to provide the safe broadband provision to schools across Britain.
- Ofcom** Office of Communications (Independent communications sector regulator)
- SWGfL** South West Grid for Learning Trust – the Regional Broadband Consortium of SW Local Authorities – is the provider of broadband and other services for schools and other organisations in the SW
- TUK** Think U Know – educational online safety programmes for schools, young people and parents.
- VLE** Virtual Learning Environment (a software system designed to support teaching and learning in an educational setting,
- WAP** Wireless Application Protocol
- UKSIC** UK Safer Internet Centre – EU funded centre. Main partners are SWGfL, Childnet and Internet Watch Foundation.