



Online Safety Policy

Version Control	
Issue/Version Number	1.3
Policy Author(s)	Deputy Head Pastoral and Boarding (DSL)
Key Staff	Head Deputy Head Pre Prep, (DDSL) Liaison Governor for Safeguarding Director of IT Head of Curriculum IT Deputy Head Academic Teaching Staff
Review Frequency	Annual
Next Review Date	Michaelmas 2027
Through School Policy	No
Policy Category	Academic and Operational
Approved By (SMT Member)	Head
Ratified By & Date (Committee)	Pastoral and Safeguarding Committee - Michaelmas 2026 (TBC)
Published (Internal and/or Web)	Internal

Online Safety Policy

1. Aims.....	3
2. Key Policy Responsibilities.....	5
3. Roles and Responsibilities	6
4. Working with Parents & Guardians.....	9
5. Filtering and Monitoring.....	10
6. Access to Digital Technology	11
7. Misuse of IT.....	12
8. Use of Technology in Curriculum.....	16
9. Record keeping and risk assessment.....	19
10. Useful online resources.....	20
11. Review and Monitoring.....	21
Links to Other School Policies.....	22
Links to External Policies, Legislation or Guidance	22
Appendix 1.....	23
Appendix 2.....	25

1. Aims

The aim of this policy is to ensure that pupils are safeguarded by an effective online safety strategy which:

- identifies online threats to the school community and protects staff and pupils from encountering any harmful or illegal material;
- provides education to the school community so that they can access and use digital technology responsibly and safely;
- will outline effective methods to identify unsafe or potentially unsafe incidents and escalate them appropriately;
- will promote a safe, inclusive and equitable online culture across the school community.

Computing covers a wide range of activities, including access to information, electronic communications and social networking. As use of technology is now universal, children need to learn computing skills in order to prepare themselves for the working environment and it is important that the inherent risks are not used to reduce children's use of technology. Further, the educational advantages of computing need to be harnessed to enhance children's learning.

The risk associated with use of technology by children can be grouped into 4 categories.

Content

The internet contains a vast store of information from all over the world which is mainly aimed at an adult audience and may be unsuitable for children.

There is a danger that children may be exposed to illegal, inappropriate, or harmful content, for example: pornography, racism, misogyny, self-harm, suicide, antisemitism, radicalisation, extremism, extreme sexual or physical violence, misinformation, disinformation (including fake news) and conspiracy theories.

Contact

Risks include being subjected to harmful online interaction with other users or generative AI applications that simulate this; 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. Chat rooms, gaming sites and other social networking sites can pose a real risk to children as users can take on an alias rather than their real names and can hide their true identity. The sites may be used by adults who pose as children in order to befriend and gain children's trust (known as "grooming") with a view to sexually abusing them.

Children may not be aware of the danger of publishing or disclosing personal information about themselves such as contact details that allow them to be identified or located. They

may also inadvertently put other children at risk by posting personal information and photographs without consent.

The internet may also be used as a way of bullying a child or for child-on-child abuse.

Conduct

Online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images including those generated by AI e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying.

Commerce

Children are vulnerable to unregulated commercial activity on the internet that could have serious financial consequences, such as fraud or identity theft, for themselves and their parents. They may give out financial information, for example, their parent's credit card details, in response to offers for goods or services without seeing the fraudulent intent. Contact via social networking sites can also be used to persuade children to reveal computer passwords or other information about the family for the purposes of fraud. Other risks include online gambling, inappropriate advertising, phishing and or financial scams.

Children may also be adversely affected by obsessive use of the internet that may have a negative impact on their health, social and emotional development and their educational attainment. They may visit sites that advocate extreme and dangerous behaviour such as self-harm or suicide or violent extremism, and more vulnerable children may be at a high degree of risk from such sites. All children may become desensitised to pornography, violence, sex and drug use or self-harm by regularly viewing these online.

Developments in artificial intelligence (AI) come with a range of benefits, including supporting learning, creativity and innovation. However, risks can include exposure to inappropriate or harmful content, exposure to inaccurate, misleading or biased content; data protection breaches; intellectual property infringements; academic integrity challenges. [Generative artificial intelligence \(AI\) in education - GOV.UK](#)

There is also growing concern for how AI can also be misused to create and share child sexual abuse material (CSAM), referred to as AI-CSAM. Under UK law, AI-CSAM is illegal. The IWF (Internet Watch Foundation) have produced this guide for professionals working with children: [ai-guidance-england-final.pdf](#)

2. Key Policy Responsibilities

- 2.1. The Deputy Head Pastoral and Boarding (DSL) is responsible for updating the Online Safety Policy and ensuring that it complies with regulations. This member of staff is the school lead in all matters pertaining to online safety (Online Safety Coordinator), including Filtering and Monitoring.
- 2.2. The Deputy Head Pastoral and Boarding (DSL), Deputy Head Academic, Deputy Head Pre Prep, Head of Curriculum IT, Deputy DSL's and Head are responsible for monitoring the implementation of the policy and maintaining appropriate records and risk assessments. These staff will also determine what actions, if any need to be taken.
- 2.3. The Deputy Head Pastoral and Boarding (DSL) is responsible for harvesting pupil voice in matters relating to online safety.
- 2.4. The policy will be reviewed annually by the Pastoral and Safeguarding Committee.

3. Roles and Responsibilities

3.1. Head's Role

- The Head has ultimate responsibility for online safety issues within the school including:
- the overall development and implementation of the School's online safety policy and ensuring the security and management of online data
- ensuring that online safety issues are given a high profile within the school community
- ensuring strong links with governors and parents/guardians to promote online safety and forward the school's online safety strategy
- ensuring online safety is embedded in staff induction and training programmes
- deciding on sanctions against staff and pupils who are in breach of Acceptable Use policies and responding to serious incidents involving online safety.

3.2. Governor's Role

- Governing bodies have a statutory responsibility for pupil safety and should therefore be aware of online safety issues, providing support to the Head in the development of the school's online safety strategy.
- Governors should ensure that there are policies and procedures in place to keep pupils safe online and that these are reviewed regularly.
- Governors should liaise with IT staff and service providers to annually review school IT filtering and monitoring systems to check their effectiveness and ensure that the Senior Management team are aware of what provision is in place and how to escalate any concerns.
- Governors should be subject to the same online safety rules as staff members and should sign an Acceptable Use Agreement in order to keep them safe from allegations and ensure a high standard of professional conduct. In particular, governors should always use school email addresses when conducting school business.

3.3. Online Safety Coordinator's role (DSL)

- Has the lead responsibility for online safety as part of their lead responsibility for safeguarding and child protection and is the Online Safety Coordinator.
- Will develop, implement, monitor and review the School's Online Safety policy.
- Will manage safeguarding incidents involving digital technology in the same manner as all other safeguarding matters (including external referrals to the Police or DDSCP) and will log appropriately.
- Will ensure that staff and pupils are aware that any online safety incident should be reported to the DSL or Deputy DSL.
- Will provide the first point of contact and advice for school staff, governors, pupils and parents.
- Liaise with key staff and the safeguarding governor to ensure the school remains up to date with online safety issues and to address any new trends, incidents and arising problems.
- Assesses the impact and risk of emerging technology and the school's response to this in association with IT staff and learning platform providers.

- Will raise the profile of online safety awareness with the School by ensuring access to training and relevant online safety literature.
- Will ensure that all staff and pupils have read and understood the Acceptable Use policy (AUP).
- Will report annually to the board of governors on the implementation of the School's online safety strategy and the annual review of the effectiveness of filtering and monitoring systems, including checks which are recorded.
- Regularly monitors the logs of incidents involving use of technology that are kept in the bullying log or in CPOMS.
- Will regularly check the monitoring and filtering online activity reports that are held in Smoothwall, in conjunction with the IT Network Manager or the Director of IT.
- Will ensure that all staff receive training (including new staff induction) in the safe use of digital technology and that they understand their roles and responsibilities in relation to filtering and monitoring so that they can help protect pupils from online dangers.
- Will ensure that all staff have appropriate data protection training at regular intervals.
- Will ensure that the staff training includes this policy, the IT Acceptable Use Policy, the Staff Employment Handbook, safeguarding information regarding the sharing of nudes and semi-nudes via image or video, cyberbullying, radicalisation and dealing with harmful online challenges or hoaxes.

3.4. The Director of IT

The Director of IT is responsible for:

- monitoring the use of digital technology across the School and suggesting developments that can be used to better ensure the online safety of pupils;
- ensuring that the School's digital infrastructure is secure and not open to malicious attack, so far as is reasonably practicable;
- ensuring that only authenticated users can access the School's technology and networks;
- monitoring systems and software to ensure that they are up to date and that they allow appropriate staff to monitor use of the internet, emails and Teams;
- keeping logs of the above which can be referred to by the Safeguarding Team;
- carrying out monitoring and audits of networks and reporting breaches to the DSL;
- supporting any subsequent investigation into breaches and preserving any evidence.
- briefing the Director of Facilities on the functionality, effectiveness and suitability of all digital technology within the school which includes the filtering and monitoring systems that are in place;
- escalating any safeguarding concerns raised by the above, to the DSL(or Deputy DSL or member of the Safeguarding team);
- ensuring that the School's filtering processes are in place, are applied and are updated on a regular basis;
- ensuring that the risks of circumvention of the safeguards outlined in this policy are minimised as much as is reasonably possible;
- ensuring that use of the School's technology is monitored to ensure compliance with this policy and that logs of suspected misuse are available to the appropriate staff so that it can be investigated via CPOMS;
- ensuring that the School's filtering and monitoring is working effectively in preventing the community from accessing any materials that pose a risk to the safeguarding of pupils. This includes any terrorist and extremist content.
- completing an annual review of the effectiveness of filtering and monitoring systems, including checks which are recorded.

- ensuring that the Filtering and Monitoring standards for schools are met; Meeting digital and technology standards in schools and colleges - Filtering and monitoring standards for schools and colleges - Guidance - GOV.UK [Meeting digital and technology standards in schools and colleges - Filtering and monitoring: core standard - Guidance - GOV.UK](#)

3.5. Role of all Repton Prep Staff

- should be positive role models for pupils with regards to online safety and should actively share their knowledge of online safety when appropriate and communicate the school's Online Safety policy and Acceptable Use policies and procedures;
- should abide by the IT Acceptable Use Policy when using digital technology;
- should report any instances of educationally valuable materials being blocked by the school's filtering and monitoring processes;
- should understand roles and responsibilities in relation to online safety generally and, filtering and monitoring specifically;
- should keep pupils safe and ensure that they receive appropriate supervision and support while using the internet;
- should report any concern about a pupil's online safety immediately to the DSL or, if unavailable, a Deputy DSL. If neither is available, follow the Safeguarding and Child Protection Policy, including direct referral or emergency action where a child is at immediate risk.

3.6. All Parents

- should promote safe use of digital technology when pupils are online;
- discuss safe usage of the internet, digital devices (such as mobile phones), social media and other online platforms with their children;
- discuss suitable adults for children to speak to if they are concerned about their online wellbeing, online safety or about the online safety of another pupil;
- should contact the DSL if they have any queries or concerns about online safety.
- will receive a copy of the termly Digital Digest information to keep them updated on relevant Online Safety issues, and the Acceptable Use Policy annually

3.7. All Pupils

- should read and sign the Repton Pupil Acceptable Use of IT agreement and ask if they have any queries or concerns;
- should understand how online safety fits into the pupil safeguarding policy and how to keep themselves safe online;
- are encouraged to contact a trusted adult if they have any queries or concerns about online safety.

4. Working with Parents & Guardians

It is essential that Repton Prep involves parents and carers in the development and implementation of online safety strategies and policies; most children will have internet access at home or own mobile devices and might not be as closely supervised in its use as they would be at school.

Therefore, parents and carers need to know about the risks so that they are able to continue online safety education at home and regulate and supervise children's use as appropriate to their age and understanding.

Repton Prep will offer online safety training opportunities and resources to parents in order to provide them with information to help them keep their child safe online.

The Head, board of governors and the Online Safety Coordinator should consider what further strategies to adopt in order to ensure parents are aware of online safety issues and support them in reinforcing online safety messages at home.

Parents should be provided with relevant information if they are asked to sign acceptable use agreements on behalf of their child so that they are fully aware of the school's expectations regarding their behaviour. Parents should also be informed that they can contact the school's DSL if they have any concerns about their child's use of technology. Where remote online learning is being used, parents should be made aware of what arrangements have been made, which websites children will be accessing and any member of staff they will be interacting with online.

5. Filtering and Monitoring

Repton Prep School demonstrates compliance through documented filtering and monitoring reports, safeguarding records of incidents and responses, supplier audits of filtering effectiveness, and regular reviews of system logs. Reports are reviewed by the DSL and shared with the Senior Management Team and Governors each term. Evidence of staff training, pupil education, and policy review is retained for inspection purposes, ensuring the school can demonstrate that filtering and monitoring measures are both effective and proportionate.

- The School uses an age-appropriate internet filtering system (Smoothwall) to block access to harmful, inappropriate, or illegal content, while ensuring that teaching and learning are not unreasonably restricted.
- Filtering provision is regularly reviewed in line with the expectations set out in *Keeping Children Safe in Education (KCSIE) 2026* and the UK Safer Internet Centre's *Appropriate Filtering and Monitoring Guidance* including an annual review of the effectiveness of filtering and monitoring systems, including checks which are recorded.
- The School ensures that filtering and monitoring systems are proportionate, balancing safeguarding needs with the requirement to provide a rich and effective educational experience.
- All internet activity on School devices and networks is monitored and logged, including searches, website access, email, and online communications, in line with KCSIE guidance and data protection policies.
- Monitoring systems are configured to generate alerts to the designated safeguarding lead (DSL and other key pastoral staff) when potential risks are identified, including cyberbullying, self-harm, radicalisation (in line with the *Prevent Duty*), grooming behaviours, or other safeguarding concerns.
- Access permissions are differentiated by role and age group (e.g., pupils, staff, visitors) to ensure safe and appropriate levels of online access.
- The School ensures governors and leaders have strategic oversight, receiving regular reports on the effectiveness of filtering and monitoring.
- All breaches, attempts to bypass filters, or concerning monitoring alerts are recorded, investigated, and escalated through the School's safeguarding procedures, in line with *Working Together to Safeguard Children (2026)*.
- Staff are trained annually (and updated as necessary) in how to respond to filtering breaches and monitoring alerts, in line with their safeguarding responsibilities under *KCSIE*.
- Staff and pupils have a responsibility to flag any occurrences when the filtering and monitoring procedures prevent access to necessary educational content. The community is trained to submit tickets with all necessary information to allow permitted content to be removed from the list of blocked websites.
- The School complies with the Prevent Duty Guidance (2023) by ensuring that online systems help to identify and restrict access to extremist content, while monitoring for indicators of radicalisation. Reference to Online Safety is stated in the Prevent Risk Assessment and staff receive training on this area.
- The Department for Education has published Generative AI: product safety expectations to support schools to use generative artificial intelligence safely, and explains how filtering and monitoring requirements apply to the use of generative AI in education. [Generative AI: product safety expectations - GOV.UK](#)

6. Access to Digital Technology

As technology continues to evolve, new devices are introduced. Wearable recording devices, including 'Smart Glasses' – eyewear that looks like ordinary spectacles but can include built-in cameras, microphones, and internet connectivity. Smart glasses can discreetly record, live-stream, or share content instantly, and therefore can pose risks to pupils, staff, and visitors. The use of smart glasses will not be permitted on school grounds by pupils, parents, visitors, or staff.

Pupils at Repton Prep are not able to have any access to mobile phones during the school day (8am to 6pm) and there are separate structures in place for use of mobile phones and technology in the boarding houses. Staff are alert to these rules, to ensure that pupils use of mobile phones is appropriate and in line with the statutory guidance on [Mobile phones in schools - GOV.UK](#)

Repton Prep demonstrates compliance through signed Acceptable Use Policies, safeguarding logs, records of breaches or misuse, filtering/monitoring reports, and staff training records. Regular reviews of device management systems, cyber security protocols, and policy updates provide further evidence for inspectors that digital technology access is safe, proportionate, and aligned with statutory requirements.

- The School provides internet access and access to the full Office 365 package inclusive of SharePoint intranet, Teams and email. Access is permitted on the basis of compliance with the IT Acceptable Use Policy. This use is monitored by the Director of IT.
- Unique login credentials are required to access any of the School's WiFi networks. Any member of the school community who thinks their login credentials have been compromised must contact the Director of IT and the service helpdesk immediately.
- Activity on the School network is secured to prevent malicious or accidental damage to systems or access to data. Monitoring is in place to notify of any attempts at such activity and this is reported in the monthly service review.
- The School has a separate WiFi network for guests and staff accommodation and this password is available upon request from The Lodge and is changed regularly.
- The School's filtering and monitoring processes will protect pupils when using the internet and this includes access to social media, when using the School's networks. However, mobile devices with mobile data will allow pupils unrestricted access to the internet.
- The School regulates mobile device usage for pupils. Staff are required to abide by the IT Acceptable Use Policy when using mobile devices.
- All online policies apply to pupils and staff both on and off the school site and any misuse of digital technologies online will be investigated appropriately.
- Staff use of personal devices for educational purposes must follow the School's safeguarding policy, including never using personal accounts or unapproved communication platforms with pupils, in accordance with KCSIE and the School's Staff Code of Conduct.
- Remote access to school systems (e.g., email, cloud platforms, homework portals) is protected by appropriate security controls, including password protection and, where possible, multi-factor authentication, in line with DfE cyber security guidance.

7. Misuse of IT

Misuse of IT includes, but is not limited to:

- Accessing, creating, storing, or sharing inappropriate, harmful, or illegal material.
- Attempting to bypass or disable the school's filtering or monitoring systems.
- Using digital technology for bullying, harassment, intimidation, or any form of abuse.
- Engaging in online behaviour that may bring the school into disrepute.
- Downloading or installing unauthorised software, applications, or files.
- Accessing another user's account, data, or files without permission.
- Deliberately introducing malware, viruses, or other harmful programs.
- Using personal devices in breach of the school's Online Safety Policy.
- Sharing personal information, images (including those generated using AI) or videos of others without consent.
- Using School systems for extremist, radicalising, or discriminatory activity (as outlined in the Prevent Duty).
- All incidents of misuse will be logged, investigated, and responded to in line with the School's safeguarding, behaviour, and disciplinary procedures.
- Serious misuse that constitutes a safeguarding concern will be immediately escalated to the Designated Safeguarding Lead (DSL) (or a Deputy DSL) and may be referred to external agencies (e.g., police, social care, Internet Watch Foundation).
- Pupils will be taught that misuse of IT is both a disciplinary and safeguarding matter, with clear age-appropriate sanctions applied.
- Staff misuse of IT will be managed under the Staff Code of Conduct, and serious breaches may result in disciplinary action, up to and including referral to the Local Authority Designated Officer (LADO) or professional bodies.
- Parents/carers will be informed of significant incidents involving their child, and support will be provided where appropriate.
- Repeated or deliberate misuse may lead to restrictions on access to digital technology, alongside restorative or educational interventions.
- The school promotes a culture of responsible reporting, encouraging pupils and staff to speak up if they become aware of misuse.
- Regular reviews of incidents will help identify patterns of misuse, ensuring the school adapts its education, supervision, and technical controls accordingly.

Pupils

Minor Misuse

These are low-level breaches of acceptable use agreements such as:

- use of non-educational sites during lessons
- unauthorised use of email
- unauthorised use of prohibited sites for instant messaging or social networking.

Sanctions will include:

- referral to the Form Tutor and the Online Safety Coordinator.
- completion of a Written Reflection (or Ref) in line with Phase 2 of the Sanctions Hierarchy and Process in the Behaviour Management Policy.

Serious Misuse

These are persistent breaches of acceptable use agreements following warnings and use of banned sites or serious breaches of online safety policy that are non-deliberate, such as:

- using/carrying an unsanctioned portable electronic device, such as a mobile phone
- online bullying (first offence)
- continued use of non-educational or prohibited sites during lessons
- continued unauthorised use of email or social networking sites during lessons
- use of file sharing software
- accidentally corrupting or destroying other people's data without notifying staff
- accidentally accessing offensive material without notifying staff.

Sanctions will include:

- referral to the Form Tutor, the Online Safety Coordinator and the Head of Year (and the Head in some cases)
- completion of an Order Mark in line with Phase 3 (or in more serious cases a Head's Detention in line with Phase 4) of the Sanctions Hierarchy and Process in the Behaviour Management Policy
- loss of internet access for a period of time
- contact with parents.

Severe/Illegal Misuse

These are deliberate actions that either negatively affect school ICT systems or are serious breaches of acceptable use agreements or anti-bullying policies, such as:

- deliberately bypassing security or access
- deliberately corrupting or destroying other people's data or violating other's privacy
- continued online bullying
- deliberately accessing, sending or distributing offensive or pornographic material

Sanctions will include:

- referral to the Form Tutor, the Online Safety Coordinator, the Head of Year and the Head.
- completion of a Head's Detention in line with Phase 4 or a temporary suspension or permanent exclusion in line with Phase 5 of the Sanctions Hierarchy and Process in the Behaviour Management Policy

- loss of access to the internet for a period of time
 - contact with parents
 - there may be a requirement to refer the incident to relevant external agencies (Policy, CEOP, Prevent, DDSCP (Derby and Derbyshire Safeguarding Children Partnership, or other local safeguarding partners)
- ongoing pastoral support will be provided to those affected.

Staff

These should reflect the seriousness with which any breach of acceptable use policies by staff members will be viewed given their position of trust and the need to ensure acceptable standards of behaviour by adults who work with children. Sanctions will be linked to the Repton Prep Staff Code of Conduct.

Minor Misuse

These are minor breaches of the school's Acceptable Use policy which amount to misconduct and will be dealt with internally as a minor IT or conduct breach in line with the Staff Code of Conduct. Any concern about an adult's conduct towards a pupil, however, small, must follow the School's low-level concerns or allegations procedure.

- excessive use of internet for personal activities not connected to professional development
- use of personal data storage media (e.g. removable memory sticks) without carrying out virus checks
- any behaviour on the world wide web and social media sites that compromises the staff member's professional standing in the school and community, for example inappropriate comments about the school, staff or pupils or inappropriate material published on social networking sites
- sharing or disclosing passwords to others or using other user's passwords
- breaching copyright or licence by installing unlicensed software.

Serious/Illegal Misuse

These infringements involve deliberate actions that undermine safety on the internet and activities that call into question the person's suitability to work with children. They represent gross misconduct that would require a strong response and possible referral to other agencies such as the police or LADO.

- serious misuse of or deliberate damage to any school computer hardware or software, for example deleting files, downloading unsuitable applications
- any deliberate attempt to breach data protection or computer security rules, for example hacking
- deliberately accessing, downloading or disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent
- receipt or transmission of material that infringes the copyright of other people or is in breach of the Data Protection Act
- bringing the Repton Prep/Repton School name into disrepute.

Possible sanctions include:

- referral to the Head, DSL, COO and Director of HR
- removal of equipment
- referral to external agencies (police, professional regulators such as TRA/DBS)
- referral to the LADO where safeguarding is implicated (KCSiE 2026 requirement)
- management under formal disciplinary procedures (may include suspension pending investigation)
- disciplinary action in line with school policies

Misuse by miscellaneous users

Anyone who has a concern about the misuse of online technology should report it immediately to the DSL or a Deputy DSL.

Concerns about possible susceptibility radicalisation must be reported to the DSL or Prevent lead. The concern will be considered using the current notice, check, share approach, and a Prevent referral will be made where appropriate. Police determine whether a referral progresses for Channel consideration. This is so that early support can be put in place to prevent vulnerable individuals from being drawn into terrorism or terrorism related activities. Any individual who has a concern relating to extremism can refer this directly to the Police.

The School has the right to withdraw access to its networks at any time.

The School will report any suspected illegal activity to the Police.

8. Use of Technology in Curriculum

- Technology is integrated across the curriculum to enhance learning and develop digital literacy.
- Pupils are guided to use digital tools safely, respectfully, responsibly, and in line with the school's online safety rules.
- Access to online resources and educational platforms is supervised and age-appropriate.
- Lessons promote digital citizenship, including safe communication, online etiquette, and awareness of potential risks.
- Filtering and monitoring systems are in place to prevent access to inappropriate content.
- Students are taught basic cybersecurity practices, including safe password management and protecting personal information.
- Staff receive training and guidance to support effective and safe use of technology in teaching.
- Parents are informed of the technologies used in the curriculum and advised on supporting safe use at home.
- The integration of technology is regularly reviewed to ensure safety, effectiveness, and alignment with educational objectives.

Pupils should be taught all elements of online safety included in the computing curriculum so that they:

- use technology safely and respectfully, keeping personal information private; identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies;
- can evaluate and apply information technology, including new or unfamiliar technologies, analytically to solve problems;
- are responsible, competent, confident and creative users of information and communication technology.

Primary pupils (EYFS to Year 6) should be taught all elements of online safety included in Statutory Relationships Education:

- about different types of bullying (including cyberbullying), the impact of bullying, responsibilities of bystanders (primarily reporting bullying to an adult) and how to get help
- 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 for others online including when we are anonymous.
- the rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them.
- how to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met.
- how information and data is shared and used online.

Statutory Health Education should include:

- that bullying (including cyberbullying) has a negative and often lasting impact on mental wellbeing
- that for most people the internet is an integral part of life and has many benefits.
- about the benefits of rationing time spent online, the risks of excessive time spent on electronic devices and the impact of positive and negative content online on their own and others' mental and physical wellbeing.
- how to consider the effect of their online actions on others and know how to recognise and display respectful behaviour online and the importance of keeping personal information private.
- why social media, some computer games and online gaming, for example, are age restricted.
- that the internet can also be a negative place where online abuse, trolling, bullying and harassment can take place, which can have a negative impact on mental health
- how to be a discerning consumer of information online including understanding that information, including that from search engines is ranked, selected and targeted
- where and how to report concerns and get support with issues online.

Secondary pupils (Years 7 and 8) should be taught all elements of online safety included in statutory Relationships and Sex Education:

- about different types of bullying (including cyberbullying), the impact of bullying, responsibilities of bystanders to report bullying and how and where to get help.
- their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online.
- about online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online.
- not to provide material to others that they would not want shared further and not to share personal material which is sent to them.
- what to do and where to get support to report material or manage issues online.
- the impact of viewing harmful content.
- that specifically sexually explicit material e.g. pornography presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners.
- that sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including jail
- how information and data is generated, collected, shared and used online.

Statutory Health Education should include:

- the similarities and differences between the online world and the physical world, including: the impact of unhealthy or obsessive comparison with others online (including through setting unrealistic expectations for body image, how people may curate a specific image of their life online, over-reliance on online relationships including social media, the risks related to online gambling including the accumulation of debt, how advertising and information is targeted at them and how to be a discerning consumer of information online
- how to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours.

Pupils with learning differences or disability may be more vulnerable to risk from use of the internet and may need additional guidance on online safety practice as well as closer supervision. Repton Prep will have a flexible and personalised approach to online safeguarding for these pupils in order to meet their needs.

The Head of Personalised Learning is responsible for providing extra support for these pupils and should:

- link with the Online Safety Coordinator to discuss and agree whether the mainstream safeguarding systems on the internet are adequate for pupils with SEND
- where necessary, liaise with the Online Safety Coordinator and the IT service to discuss any requirements for further safeguards to the school IT system or tailored resources and materials in order to meet the needs of pupils with SEND
- ensure that the school's Online Safety policy is adapted to suit the needs of pupils with SEND
- be aware that some pupils with SEND may not have the cognitive understanding to differentiate between fact and fiction online and may repeat content and behaviours in the real world without understanding the consequences
- liaise with parents, carers and other relevant agencies in developing online safety practices for pupils with SEND
- keep up to date with any developments regarding emerging technologies and online safety and how these may impact on pupils with SEND.

9. Record keeping and risk assessment

Repton Prep School consistently reviews the potential risks associated with all online activities, platforms, and digital tools, which are regularly updated. All online safety incidents and concerns are promptly recorded, with actions taken and outcomes noted. Records are securely stored, accessed only by authorised staff, and used to monitor trends, evaluate safety measures, and guide improvements. Risk assessments inform action plans to address vulnerabilities, and staff are trained to recognise risks and report concerns. Relevant information may be shared with parents when appropriate, and all practices comply with statutory safeguarding and school policy requirements.

- All online activities, platforms, and digital tools are subject to documented risk assessments to identify potential hazards. These are held by the Director of IT at Repton.
- The DSL (or a Deputy DSL) will carry out risk assessments where a concern about a pupil's safety has been identified and appropriate action will be taken. Staff are trained to recognise risks and report concerns in accordance with school policies;
- Risk assessments are regularly reviewed and updated to reflect new technologies, identified risks, or changes in practice.
- Any online safety incidents or concerns are promptly recorded, detailing the actions taken and outcomes, and are logged on CPOMS.
- Records are used to monitor trends, evaluate safety measures, and inform improvements to online safety practices.
- All records are stored securely, accessed only by authorised personnel, and managed in line with data protection requirements.
- Risk assessments guide the development of action plans to address vulnerabilities and strengthen safeguards.
- Staff are trained to recognise risks, maintain accurate records, and report concerns in accordance with school policy.
- Where appropriate, relevant information may be shared with parents to support a collaborative approach to online safety.
- Record keeping and risk assessment practices comply with statutory safeguarding requirements and school policy standards.

10. Useful online resources

Useful resources for staff

- [Keeping children safe in education - GOV.UK \(www.gov.uk\)](http://www.gov.uk)
- [Homepage - UK Safer Internet Centre](#)
- [Keeping children safe online | NSPCC](#)
- [The Prevent duty: safeguarding learners vulnerable to radicalisation - GOV.UK \(www.gov.uk\)](http://www.gov.uk)
- [UK Safer Internet Centre provides an online safety helpline for professionals at 0344 381 4772 or helpline@saferinternet.org.uk.](mailto:helpline@saferinternet.org.uk)
- [Channel and Prevent Multi-Agency Panel \(PMAP\) guidance - GOV.UK \(www.gov.uk\)](http://www.gov.uk)
- [Harmful online challenges and online hoaxes - GOV.UK \(www.gov.uk\)](http://www.gov.uk)
- [Eliminating Child Sexual Abuse Online – Internet Watch Foundation \(iwf.org.uk\)](http://iwf.org.uk)
- [The use of social media for online radicalisation - GOV.UK \(www.gov.uk\)](http://www.gov.uk)
- [Sharing nudes and semi-nudes: advice for education settings working with children and young people - GOV.UK \(www.gov.uk\)](http://www.gov.uk)
- [Myth vs Reality: PSHE toolkit | Childnet](#)
- [Preventing bullying - GOV.UK \(www.gov.uk\)](http://www.gov.uk)
- [Educateagainstthate – Provides practical advice and support on protecting children from extremism and radicalisation](#)
- [National Crime Agency's CEOP Education Programme provides resources for professional's and parents and carers on protecting children and young people from online child sexual abuse.](#)

Useful resources for parents

- Online Safety Policy
- [Parents and Carers Toolkit | Childnet](#)
- [Information, Advice and Support to Keep Children Safe Online \(internetmatters.org\)](http://internetmatters.org)
- [Keeping children safe online | NSPCC](#)

Useful resources for pupils

- [CEOP Education \(thinkuknow.co.uk\)](http://thinkuknow.co.uk)
- [CEOP Safety Centre](#)
- [Children and young people - UK Safer Internet Centre](#)

11. Review and Monitoring

This policy is reviewed on an annual basis and is updated in accordance with changes to guidance and developments in best practice using the listed sources of information.

This policy is reviewed by the Pastoral and Safeguarding Committee.

Links to Other School Policies
Staff Employment Handbook
Safeguarding Children and Child Protection Policy
Data Protection Policy
Wellbeing Policy
IT Acceptable Use Policy
Anti-Bullying Policy
PSHE and RSE Policy
Pupil Supervision Policies
Pupil Behaviour Management Policy
EDIB and Equal Opportunities Policy
Health and Safety Policy Statement
Pupil Code of Conduct
Staff Code of Conduct and Whistleblowing Policy
Visitors and Visiting Speaker Policy

Links to External Policies, Legislation or Guidance
Keeping Children Safe in Education (DfE, 2026)
Prevent duty guidance for England and Wales (Home Office, 2023)
Searching, screening and confiscation: advice for schools (DfE, 2022)
Preventing and tackling bullying (DfE, 2017)
Sharing nudes and semi-nudes (DfE, 2020), Channel duty guidance (Home Office, 2020)
Relationships, Education, Relationships and Sex Education and Health Education guidance (DfE, 2026)
Teaching online safety in school (DfE, 2019)
Harmful online challenges and online hoaxes (DfE, 2021)
Working Together to Safeguard Children (2026)

Appendix 1: Acceptable Use Policy for pupils in EYFS to Year 4



Acceptable Use Policy for Pupils in EYFS to Year 4

Pupil's Name:
Form:

1. My promises when using technology

When I use a computer, tablet or the internet at school, I will:

- use only the computers, tablets, websites, apps and accounts my teacher has chosen. I will ask before trying something new;
- keep my password secret. I will tell an adult if I think someone else knows it;
- be kind and polite in messages, games and work we share. I will not send anything to upset someone;
- tell an adult I trust straight away if I see something that worries or confuses me. If someone is unkind, if someone sends me a message I do not like or if someone I do not know sends me a message, I will not reply or pass it on;
- keep private details safe. This includes my full name, where I live, my school, phone numbers and passwords. I will not share someone else's private details. I will ask an adult before sharing anything online;
- only send messages or emails when my teacher says I can, using my school account. I will never arrange to meet someone I know only from online;
- **not** use AI tools, such as chatbots or picture makers. If I open one by mistake or someone asks me to use one, I will tell my teacher. I will not put anyone's name, photo or private details into AI;
- ask an adult I trust if I am not sure whether a picture, video, message or news story is real. AI can make or change these things;
- only take photos, videos or sound recordings when my teacher asks me to. I will not record, livestream or share pictures or sounds of other pupils or adults without permission. This includes using a phone, watch, camera or recording glasses, such as Meta smart glasses;
- tell a teacher if I open something by mistake, do something wrong, or see someone break these promises. I can ask for help and will not be blamed for telling.

Teachers may check what I do on school accounts and devices to help keep me safe. The school also checks online activity. I can always tell an adult if something goes wrong.

2. For parents and carers

I have talked about these promises with my child in a way they can understand. I agree that my child may use school technology and the internet for learning, with adult supervision and in line with school expectations. I understand that Repton Prep uses filtering, monitoring and supervision, but unwanted content may still appear. I will tell the school if I have an online safety concern about my child.

Parents have been sent a copy of the acceptable use agreement above and agreement is assumed, unless parents contact the school directly.

3. Publication preference

The School will assume consent for children's work to be published on the school website, in school publications and on official school social media for school communications and promotion, but parents always have the option to opt out.

For school staff: Record the parent's choice alongside their image permissions. Follow school safeguarding and online safety procedures if a concern is raised. Review this agreement each year.

The details of this AUP are also sent to parents annually.

Appendix 2: Acceptable Use Policy for pupils in Years 5 to 8



Acceptable Use Policy for Pupils in Years 5 to 8

The pupil element of this form is completed as an online form each academic year. Pupils joining the school at other times in the academic year are prompted to complete it when they access the school IT system for the first time.

General statement

The computers are provided and maintained for the benefit of all children, who are encouraged to use and enjoy these resources, and ensure they remain available to all. Pupils are responsible for good behaviour on the Internet just as they are in a classroom or around school. The Repton Prep Code applies. Remember that access is a privilege, not a right, and inappropriate use will result in that privilege being withdrawn.

☐ I agree to use the Repton Prep IT network

Equipment

- Do not install, attempt to install or store programs of any type on the computers without permission.
- Do not damage, disable, or otherwise harm the operation of computers, or intentionally waste resources.
- Do not open files brought in on removable media (such as floppy disks, CDs, USB drives etc.) until they have been checked with antivirus software and been found to be free of viruses.
- Do not connect mobile equipment to the network (e.g. laptops, tablet PCs, PDAs etc.) until they have been checked with antivirus software and been found to be free of viruses.
- Do not eat or drink near computer equipment.

☐ I have read this. I agree and understand.

Security and privacy

- Do not disclose your password to others, or use passwords intended for the use of others.
- Never tell anyone you meet on the Internet your home address, your telephone number, any details about school, or send them your picture.
- Do not use the computers in a way that harasses, harms, offends or insults others.
- You must not take, store or send images or recordings of any kind, of fellow pupils or staff without their permission or knowledge.

- Respect, and do not attempt to bypass, security in place on the computers, or attempt to alter the settings.
- Computer storage areas and web accounts will be treated like school desks. Staff may review files and communications to ensure that users are using the system responsibly.

☐ I have read this. I agree and understand.

Using the Internet and AI

- The Internet should only be used for study or for school authorised/supervised activities.
- Pupils should not use open generative AI in school due to age restrictions.
- Do not use the Internet or online accounts to obtain, download, send, print, display or otherwise transmit or gain access to materials which are unlawful, obscene or abusive.
- Respect the work and ownership rights of people outside the school, as well as other pupils or staff. This includes abiding by copyright laws.
- Do not engage in 'chat' activities over the Internet. This takes up valuable resources which could be used by others to benefit their studies.
- Never arrange to meet anyone via the Internet. People you contact online are not always who they seem.

☐ I have read this. I agree and understand.

Email and messaging

- Be polite and appreciate that other users might have different views from your own.
- The use of strong language, swearing or aggressive behaviour is not allowed.
- Never open attachments to emails unless they come from someone you already know and trust. They could contain viruses or other programs which could destroy information and software on the computers.
- The sending or receiving of emails containing material likely to be unsuitable for children or schools is strictly forbidden. This applies to any material of a violent, dangerous, racist, or inappropriate content.
- Always report such messages to a member of staff.

☐ I have read this. I agree and understand.

Enforcement

This document is to be read carefully by all pupils. If any child disobeys these provisions, access to the Internet will be denied and sanctions may be issued in line with the Online Safety Policy.

☐ I agree to use the IT network safely and responsibly.

The details of this AUP are also sent to parents annually.