Boundary Oak School

Online Safety Policy

2026 - 2027

PERSON RESPONSIBLE FOR THE LATEST REVISION	Head of School, DSL & Head of IT
LAST REVIEW	October 2026
Advisory Board sign off	November 2026
NEXT REVIEW	September 2027

1) OVERVIEW

This policy replaces the Boundary Oak E-Safety Policy (November 2025). It has been restructured around the Hampshire / SWGfL model online safety policy (roles, education, technical, data protection, communications and incident response) and updated to reflect Keeping Children Safe in Education (KCSIE) 2026, which came into force on 1 September 2026. A summary of the main changes is set out below.

Summary of Key Changes 2026-27

- Terminology - "E-safety" replaced by "online safety" throughout, in line with KCSIE and DfE guidance. "Nudes and semi-nudes" used consistently, including AI-generated and digitally altered images.
- The four Cs - Updated to the KCSIE 2026 definitions: content now includes misinformation, disinformation and conspiracy theories; contact includes harmful interaction with generative AI that simulates human interaction; conduct includes AI-generated explicit images; commerce includes phishing and financial scams.
- Filtering and monitoring - A named SLT member is responsible for filtering and monitoring. Their review, supported by the DSL and IT, takes place at least once every academic year and records are kept of checks on all internet-connected devices in all relevant locations.
- DSL role - The DSL's lead responsibility for understanding filtering and monitoring is explicit and must be reflected in the DSL job description.
- Generative AI - New section on generative AI, linked to the DfE Generative AI product safety expectations and the school's AI Policy.
- Cyber security - Cyber security recognised as a safeguarding issue, referencing the DfE Cyber security standards for schools and colleges.
- Mobile phones - The school is a mobile-phone-free environment during the school day by default, in line with the statutory Mobile phones in schools guidance.
- Staff reading - All staff read KCSIE Part One in full and Annex A. Training includes filtering and monitoring roles and how to escalate concerns.
- Systems - Technical references updated to the current BOS stack (Smoothwall, Fortigate, Classroom.cloud, Heimdal, TrendMicro, RedStor, MyConcern).
- Appendices - New incident flowchart, filtering and monitoring check log, UK online safety portals for staff, pupils and parents, and an updated glossary of acronyms. The out-of-date apps list has been replaced.

School Aims and Objectives

Aims

- To safeguard and promote the welfare of pupils and staff, online and offline.
- To ensure the security and confidentiality of school systems and personal data.
- To safeguard the school's facilities and support positive pupil behaviour.
- To provide pupils with a safe, high-quality digital experience as an essential part of their learning.
- To develop a good understanding of research skills and the need to avoid plagiarism and uphold copyright.
- To develop a good understanding of artificial intelligence (AI), including its benefits and risks (see the school's AI Policy).

Objectives

- To provide high-quality, appropriately filtered and monitored internet access for all pupils and staff.
- To promote the welfare of all pupils through clear communication of expectations, protocols and procedures for all users of technology.
- To rigorously monitor and review technology use and practice by all users, and to record and act on what we find.
- To teach pupils what internet use is acceptable and what is not, and give clear expectations for safe and respectful behaviour online.
- To educate pupils in effective and critical use of the internet, including locating, retrieving and evaluating information and recognising misinformation and disinformation.
- To ensure that the use of internet-derived material by staff and pupils complies with copyright law.
- To make explicit to pupils, staff and parents the procedures for reporting inappropriate, harmful or illegal content and behaviour, including content relating to terrorism, extremism and violence.

2) SCOPE AND GENERAL STATEMENT

Boundary Oak School recognises the benefits and opportunities which new technologies offer to teaching and learning. We encourage the use of technology to enhance skills and promote achievement. However, the accessible and global nature of the internet and the variety of technologies available mean that we are also aware of the potential risks and challenges associated with such use. Our approach is to implement safeguards within the school and to support staff and pupils to identify and manage risks independently. We believe this can be achieved through a combination of security measures, training, guidance and the implementation of our associated policies.

In line with our duty to safeguard pupils under KCSIE 2026, we take a whole-school approach to online safety which empowers us to protect and educate pupils and staff in their use of technology, and which establishes mechanisms to identify, intervene in and escalate any concern where appropriate. Online safety is an integral part of safeguarding and is considered alongside our Relationships, Sex and Health Education (RSHE), behaviour, mobile phone and staff training arrangements.

This policy applies to all pupils (including boarders and EYFS), staff, volunteers, contractors, visitors and members of the school community who have access to school IT systems, both on the premises and remotely, and to the use of school-owned devices and services off site. It applies to all use of the internet and electronic communication, including email, messaging, mobile phones, smart devices, games consoles, social media and AI tools. Any user of school IT systems must agree to the relevant Acceptable Use Policy (AUP) before access is granted.

Related School Policies

This policy should be read in conjunction with: Safeguarding and Child Protection Policy; Child-on-Child Abuse Policy; Behaviour Policy; Anti-Bullying (including Cyber-Bullying) Policy; Safeguarding Pupils Vulnerable to Radicalisation (Prevent) Policy; IT Acceptable Use Policies (staff, pupil, parent and visitor); Mobile Phone Policy; AI Policy; Data Protection Policy and Privacy Notices; Taking, Storing and Using Images of Pupils Policy; Staff Code of Conduct; Boarding Policy; RSHE Policy; and the Whistleblowing Policy.

Legislation and statutory guidance

- Keeping Children Safe in Education 2026 (DfE, in force from 1 September 2026), read alongside Working Together to Safeguard Children.
- Filtering and monitoring standards for schools and colleges and Cyber security standards for schools and colleges (DfE).
- Generative AI: product safety expectations and Generative artificial intelligence in education (DfE).
- Mobile phones in schools (statutory from 1 September 2026, following section 36 of the Children's Wellbeing and Schools Act 2026).
- Sharing nudes and semi-nudes: advice for education settings (UKCIS).
- Teaching online safety in schools and Education for a Connected World (DfE / UKCIS).
- Prevent duty guidance and Searching, screening and confiscation (DfE / Home Office).
- Online Safety Act 2023; UK GDPR and the Data Protection Act 2018; Computer Misuse Act 1990; Education and Inspections Act 2006; Children Act 1989; Equality Act 2010; and the EYFS statutory framework.

3) UNDERSTANDING ONLINE RISK

The internet is an essential element of life for education, business and social interaction. The school has a duty to provide pupils with quality internet access as part of their learning, and to help them understand and manage the risks that come with it. KCSIE 2026 groups online risk into four areas, known as the four Cs:

Content

Being 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

Being subjected to harmful online interaction with other users, or with generative AI applications that simulate human interaction (such as AI chatbots and companion apps). 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 (including those generated using AI) and online bullying.

Commerce

Risks such as online gambling, inappropriate advertising, phishing and financial scams. Where pupils, students or staff are at risk, phishing can be reported to the Anti-Phishing Working Group, and suspicious emails to the NCSC at report@phishing.gov.uk.

These risks come into play at different stages of a child's development, so vulnerability is not static. It needs to be understood in the broader context of children's lives and their stage of emotional, psychological and physical development, especially as children enter puberty. Online and offline harm are often intertwined, and abuse can take place online, face to face, or both at the same time. The absence of reports does not mean that online harm is not happening.

Spectrum of Vulnerability



Our aim is always to help children and young people become as resilient as possible by talking with them, taking an interest in what they are doing online, and developing our own awareness of their online behaviours and habits. If we can describe and explain a risk, we are in a better position to reduce it.

Emerging risks for 2026–27

- Generative AI: AI chatbots and companion apps that simulate friendship or relationships; AI-generated misinformation; and tools used to create AI-generated or "deepfake" nude images of real people, including peers and staff.
- Sextortion: financially motivated sexual extortion, where a young person (frequently a teenage boy) is tricked or coerced into sharing an image and then blackmailed for money.
- Misogyny, extremism and radicalisation: online influencers and algorithm-driven content that normalise misogyny, hate or extremist ideas.
- Gambling and gambling-like features: loot boxes, skin betting and in-game spending.
- Cyber crime: phishing, account takeover and scams targeting pupils, parents and staff.

Indicators that a child may be at risk online

- Spending increasing amounts of time online, or becoming secretive or anxious about their device, and spending less time with school, family or local friends.
- Being unwilling to share or show online contacts, or having new contacts or a new "friend" or relationship that began online.
- Arranging to meet people they have met online, including through gaming platforms, chat sites or social media.
- Receiving gifts, money, gaming credit or in-game currency from someone they do not know.
- Exchanging, or being pressured to exchange, images or videos, including via webcam or livestreaming, or concern that images of them are being circulated.
- Sudden changes in mood, sleep or behaviour, or signs of distress after using a device, which may indicate bullying, sextortion or exposure to harmful content.
- Forming a strong emotional attachment to an AI chatbot or companion app.
- Unexplained money, spending or debt, or use of adult content-subscription sites.

Safeguarding is everyone's business. Where there are concerns about a child's wellbeing, staff should consider online harms alongside the traditional categories of abuse (physical, emotional and sexual abuse and neglect). Online abuse must never distract us from the very real, and still more common, harm caused by family members, friends and associates.

4) ROLES & RESPONSIBILITIES

There are clear lines of responsibility for online safety within the school. Any member of staff with a concern should report it to the DSL (or a Deputy DSL) without delay. Technical issues are reported to the IT team via the IT helpdesk.

4.1 Proprietor (Globeducate) and the Advisory Board

- Hold the school to account for the implementation of this policy and ensure it is reviewed at least annually.
- Ensure appropriate filtering and monitoring systems are in place, that their effectiveness is reviewed at least once every academic year, and that the school can demonstrate that these reviews have taken place.
- Ensure that the school meets the DfE filtering and monitoring standards and cyber security standards.
- Take part in online safety training and awareness sessions, including on filtering and monitoring.

4.2 Headteacher

- Has overall responsibility for the safety (including online safety) of all members of the school community.
- Ensures that the DSL, the SLT lead for filtering and monitoring and the IT team have the time, training and resources to carry out their roles.
- Is informed of, and responds to, any allegation of misuse by a member of staff, in line with the Safeguarding Policy and the allegations management procedures (including referral to the LADO where the threshold is met).

4.3 SLT member responsible for filtering and monitoring

- Is named on the front of this policy and in the Safeguarding Policy.
- Leads the review of filtering and monitoring at least once every academic year, supported by the DSL and IT, and whenever a safeguarding risk is identified or there is a change in working practice, systems or IT provider.
- Ensures that a record is kept of the review and of the regular checks, and reports the outcome to the Proprietor and Advisory Board.
    - Undertakes training so that they understand the DfE filtering and monitoring standards and what the school's systems can do.

4.4 Designated Safeguarding Lead (DSL) and Deputies

The DSL takes lead responsibility for safeguarding and child protection, including online safety and understanding the filtering and monitoring systems and processes in place. This is reflected in the DSL's job description. The DSL should be trained in online safety and be aware of the potential for serious child protection and safeguarding issues to arise from:

- sharing of personal data; access to illegal or inappropriate material; inappropriate online contact with adults or strangers;
- potential or actual grooming, sexual or criminal exploitation, and sextortion;
- online bullying, online sexual harassment and the creation or sharing of nudes and semi-nudes (including AI-generated images);
- radicalisation and extremism; and harmful interaction with AI applications.

The DSL liaises with the Head of IT and the Headteacher on filtering and monitoring, reviews alerts and reports, and ensures concerns are recorded and acted upon on MyConcern.

4.5 Online Safety Team

The Online Safety Team consists of the DSL, the Headteacher, the SLT lead for filtering and monitoring and the Head of IT. It meets at least termly, reviews filtering and monitoring reports and incident trends, and keeps its records on the Online Safety SharePoint site.

4.6 Head of IT and technical staff

Those with technical responsibilities are responsible for ensuring that:

- the school's technical infrastructure is secure and is not open to misuse or malicious attack;
- the school meets the DfE filtering and monitoring standards, the cyber security standards and any Globeducate group IT policy that applies;
- users may only access networks and devices through a properly enforced password policy, with multi-factor authentication (MFA) for staff and administrative accounts;
- filtering and monitoring systems are applied to new devices and services before they are released to staff and pupils, and that changes to filtering are logged and authorised by the DSL;
- they keep up to date with online safety technical information and report any suspected misuse or problem to the DSL.

4.7 Teaching and support staff (including volunteers)

Are responsible for ensuring that they:

- have read KCSIE Part One in full and Annex A, and have an up-to-date awareness of online safety matters and of this policy;
- have read, understood and signed the Staff Acceptable Use Policy and Staff Code of Conduct;
- understand their role in filtering and monitoring, including supervising pupils' use of devices and reporting any concern or any content that should have been blocked;
- embed online safety in their teaching and model safe, responsible and professional behaviour online;

- carry out all digital communications with pupils and parents on a professional level and only through official school systems;
- report any suspected misuse, problem or concern to the DSL without delay, and never guarantee confidentiality to anyone reporting an incident.

4.8 Boarding staff

Boarding staff supervise boarders' use of personal devices during tech time, manage the secure storage of devices overnight (see section 11) and report concerns to the DSL.

4.9 Pupils

- Are responsible for using school digital technology systems in accordance with the Pupil Acceptable Use Agreement, which they sign annually.
- Should attend and take part in online safety lessons, know how to report concerns and seek help when they are worried about themselves or someone else.
- Must act safely and responsibly at all times when using the internet, AI tools and mobile technologies, both in and out of school, where their behaviour affects members of the school community.

4.10 Parents and carers

- Support the school in promoting online safety and sign the Parent Acceptable Use Policy annually.
- Talk with their children about their online lives, including the sites and apps they use and who they talk to when away from school.
- Follow the school's guidance on photographs, social media and communication with staff.

4.11 Visitors, contractors and community users

Anyone not directly employed by the school, including summer school and lettings users, must agree to the Visitor / Guest Acceptable Use Policy before being given access to the internet on site. All use of the school internet connection by community and other organisations must be in accordance with this policy.

5) EDUCATION - PUPILS

Online safety is a focus in all areas of the curriculum and staff reinforce online safety messages wherever relevant. The online safety curriculum is broad, relevant and progressive, mapped to Education for a Connected World and delivered through Computing, PSHE and RSHE, using resources such as ProjectEVOLVE and CEOP Education. It is provided in the following ways:

- A planned online safety curriculum as part of Computing, PSHE and RSHE lessons, regularly revisited and adapted to the age and needs of pupils, including those with SEND.

- Key messages reinforced through assemblies, tutor time, boarding and pastoral activities, and events such as Safer Internet Day.
- Pupils are taught to be critically aware of the content they access online, to check the accuracy of information, and to recognise misinformation, disinformation and conspiracy theories.
- Pupils are taught to acknowledge the source of information and to respect copyright, and how to use AI tools honestly and safely.
- Pupils are taught about consent, healthy relationships and the law around nudes and semi-nudes, and that AI-generated images of real people can be just as harmful.
- Pupils are supported in building resilience to radicalisation through a safe environment in which to debate controversial issues.
- Prep and Senior pupils are made aware, in an age-appropriate way, of the dangers of pornography, violent content, extremist views, gambling and scams.

What we teach children and young people

1. Guard your information: set privacy settings and protect your address, phone number, school, passwords and location. Turn off location sharing unless you need it.
2. Limit time online: log off and take time for family and face-to-face time with friends.
3. Friend or foe? Not everyone online is who they say they are. Never meet an online-only "friend" offline, and tell a trusted adult if someone tries to.
4. Talk about it: tell a trusted adult about anything that upsets you or makes you uncomfortable. Just because it is online doesn't mean it is true.
5. Webcams and livestreams: never use random video-chat sites, and never do anything on camera you wouldn't want shared.
6. Nudes: never send, ask for or share nude images, including AI-made ones. If it has happened, it is not too late to get help – use Report Remove and talk to an adult.
7. AI chatbots: an AI is not a friend or a counsellor; don't share personal information with it and check what it tells you.
8. Be scam smart: don't open strange messages or links, and beware "free" downloads, giveaways and anyone asking for money or codes.
9. Don't be a pirate: don't download music, films or games illegally – it risks viruses and identity theft.
10. Teamwork: help each other, look out for friends and know when to log off.

Online bullying – what we teach children

Don't respond or retaliate; talk to a trusted adult; save the evidence; block and report the bully; don't be a bully; and be a friend, not a bystander.

Online bullying – what adults should do

Listen and take the child seriously; make sure the child is safe and feels safe; don't overreact; encourage the child not to retaliate; gather the facts and save the evidence (but never copy or forward images of a child); involve the child in solving the problem; build self-esteem and resilience; and contact the school if the bullying involves other pupils.

6) EDUCATION & TRAINING – STAFF, VOLUNTEERS & ADVISORY BOARD

It is essential that all staff receive online safety training and understand their responsibilities as outlined in this policy. Training will be offered as follows:

- All new staff receive online safety training as part of their induction, including KCSIE Part One and Annex A, this policy and the acceptable use agreements.
- A planned programme of online safety training (National College courses, in-house training and one-to-one support where needed) is updated and reinforced regularly, at least annually, as part of safeguarding training.
- Training includes an understanding of the expectations, roles and responsibilities around filtering and monitoring, and how to escalate concerns.
- Training covers emerging risks including generative AI, sextortion, nudes and semi-nudes, and cyber security (phishing awareness and safe password use).
- An audit of the online safety training needs of all staff is carried out regularly, and records of training are kept.
- The DSL and Deputies receive enhanced online safety training at least every two years, with regular updates in between.
- Members of the Advisory Board take part in online safety and filtering and monitoring training and awareness sessions.

7) ENGAGING PARENTS & CARERS

- Parents' attention is drawn to this policy in newsletters, the school website and the admissions pack.
- Parents have access to the Boundary Oak E-Safety website, which has information and guidance on staying safe online, the latest version of this policy and any forms that need to be signed.
- All new parents sign the Parent Acceptable Use Policy and the pupil online safety rules when their child joins the school, and re-confirm these annually.
- The school holds regular online safety forums and shares termly updates on current risks.
- The school talks with parents about what their children are being asked to do online, which sites they will access and who they will interact with, including during remote learning and when away from school.
- Practical guidance for parents is set out in Appendix 4, and recommended UK support services in Appendix 3.

8) TECHNICAL – INFRASTRUCTURE, FILTERING & MONITORING

8.1 Infrastructure and information system security

- School technical systems are managed so that the school meets the DfE digital and technology standards, including the cyber security standards.
- There are regular reviews and audits of the safety and security of school technical systems.
- Servers, wireless systems and cabling are securely located and physical access is restricted.
- All users have clearly defined access rights to school systems and devices, and are provided with a username and secure password. Users are responsible for the security of their credentials. MFA is enforced for staff and administrative accounts.
- Endpoint protection (Heimdal and TrendMicro) is installed and updated automatically on all school devices; operating systems and applications are patched promptly.
- The perimeter is protected by a Fortigate firewall. The BOSStaff and BOSBYOD wireless networks are separated and filtered.
- School data is backed up securely (RedStor), with backups tested and protected from ransomware.
- Personal data must not be sent over the internet or taken off site unless it is encrypted or otherwise secured (see section 14).

8.2 Filtering

- Internet access is filtered for all users on all school networks and school-owned devices, including devices used off site, using Smoothwall web filtering.
- Filtering blocks illegal content (including child sexual abuse material on the IWF list and unlawful terrorist content), and age-appropriate filtering rules are applied to different user groups (EYFS / Pre-Prep, Prep, Senior, boarders, staff and guests).
- Filtering is applied to generative AI tools in line with the DfE Generative AI product safety expectations. Only AI tools approved by the school may be used with pupils.
- The school takes care that filtering does not "over-block" and unreasonably restrict teaching and learning. Requests to unblock sites are made through the IT helpdesk and approved by the DSL.
- If staff or pupils come across unsuitable material, it must be reported immediately to the DSL and the IT team. Pupils in Reception to Year 6 report to their class teacher or form tutor; pupils in Years 7–11 can also use the "Report suspicious activity online" button on the pupil Useful Links page. Staff have an equivalent button on the staff Useful Links page.

8.3 Monitoring

- Web activity is monitored by Smoothwall, which sends the Online Safety Team daily safeguarding reports of concerning searches and a weekly report of blocked searches. The DSL reviews the keyword lists so that they can be updated as safeguarding risks change.
- Pupil devices in lessons are monitored through Classroom.cloud, and staff physically supervise pupils' use of devices. Staff alert the DSL and IT team to any inappropriate use or content.
- Incoming and outgoing email is monitored through the Outlook monitoring group, and a library of "flagged" words is maintained.
- Email and web alerts that raise an issue are discussed by the DSL and the Head of IT and, where relevant, the Headteacher or SLT, dealt with according to severity and recorded on MyConcern and the Online Safety SharePoint.
- All users are told that school network and internet use is monitored and can be traced to the individual user.

8.4 Checks, annual review and records

- The DSL and the Head of IT carry out monthly checks that filtering and monitoring are working as expected and have not been changed or deactivated. Checks cover school-owned devices and services (including those used off site), all relevant locations (classrooms, boarding house, staff areas, guest Wi-Fi) and a range of user groups (pupils, staff, boarders and visitors), using tools such as the SWGfL Test Filtering service.
- The SLT lead for filtering and monitoring leads a full review at least once every academic year, supported by the DSL and IT, using the DfE filtering and monitoring standards and the school's

risk profile. A review is also carried out when a safeguarding risk is identified or there is a change in working practice, systems or IT provider.

- A record is kept of every check and review, including when it took place, who carried it out, which devices, locations and user groups were tested, any issues identified and the actions taken. The template at Appendix 2 is used. Records are stored on the Online Safety SharePoint and made available to the Proprietor, the Advisory Board and inspectors.
- The Proprietor reviews the standards with the Online Safety Team and service providers to ensure they are met.

8.5 Bring Your Own Device (BYOD) and boarders' devices

- BYOD laptops are permitted only for pupils in the year groups set out in the Pupil IT Acceptable Use Policy (Year 9 and above), and only if they are not 4G/5G or mobile-hotspot enabled.
- Every BYOD device must be checked by the IT team before first use to make sure no VPN, proxy or malicious apps or extensions are installed. The school's filtering certificate is then installed so that traffic on the BOSBYOD network is filtered and monitored. Pupils sign in to BOSBYOD with their school username and password; devices without the certificate, or users not in the BYOD group, cannot connect.
- Boarders' phones and tablets connect to BOSBYOD with the same certificate. Boarders have a separate, time-based filter group which is slightly more relaxed after 5.30pm (to allow, for example, video calls home and age-appropriate social media) and reverts to the pupil rules at 6.30am.
- Pupils signing in to BOSBYOD agree, through the annual Pupil IT Rules, that all browsing is monitored. Tablets are not permitted in school without the written permission of the Headteacher.

8.6 Cyber security

Cyber security is a safeguarding issue: compromised safeguarding records, stolen pupil data or a cyber incident can directly harm children. The school follows the DfE cyber security standards, trains staff to recognise phishing and social engineering, maintains an incident response plan and reports cyber incidents to the Head of IT and DPO immediately. Fraud and cyber crime are reported to Action Fraud and, where personal data is affected, to the ICO (see section 14).

9) GENERATIVE ARTIFICIAL INTELLIGENCE (AI)

AI offers real benefits for teaching, learning and administration, but KCSIE 2026 recognises AI as a safeguarding issue. This section should be read with the school's AI Policy.

- Only AI tools that have been risk-assessed by the Head of IT and DSL, subject to a Data Protection Impact Assessment (DPIA) where personal data is involved, and approved at Globeducate group level may be used with pupils or with school data.
- Approved AI tools must meet the DfE Generative AI product safety expectations, including appropriate filtering, monitoring, age-appropriate design and protection against harmful content.
- Staff must not enter personal data, safeguarding information or confidential school information into public AI tools.
- Pupils are taught to use AI honestly (avoiding plagiarism), to check AI output for accuracy and bias, and that AI chatbots and companions are not people, friends or counsellors.
- Creating, sharing or threatening to share AI-generated or digitally altered sexual images of any person – pupil or adult – is treated as a serious safeguarding and behaviour matter. Where the image depicts a child, it is handled as a nudes and semi-nudes incident (section 16).
- Misuse of AI to impersonate, bully or harass others, including deepfakes of staff, is dealt with under the Behaviour and Anti-Bullying policies, and may be reported to the police.

10) MOBILE TECHNOLOGIES & MOBILE PHONES

- In line with the statutory Mobile phones in schools guidance, Boundary Oak is a mobile-phone-free environment during the school day. Pupils' mobile phones, and smartwatches or other devices with cameras, messaging or data connections, must not be used during the school day. Any exceptions (for example a medical need such as glucose monitoring, or a SEND need) are agreed in writing by the Headteacher. Full arrangements are set out in the Mobile Phone Policy.
- Devices brought to school in breach of the Mobile Phone Policy may be confiscated and returned in line with the Behaviour Policy. Staff may search for banned items in accordance with Searching, screening and confiscation guidance.
- The sending of abusive, threatening or inappropriate messages or images by any means is forbidden.
- Staff use a school phone where contact with pupils or parents is required. Staff mobile phones may be used for registration on iSAMS or SOCS and to communicate with colleagues (for example on ChatPro) for logistical or emergency purposes where no landline is available. Personal devices must not be used in EYFS settings.
- The school acceptable use agreements for staff, pupils and parents set out the expectations for the use of mobile technologies.

11) BOARDING

- Year 10 and 11 boarders may have their devices from 4.30pm to 5.30pm if they are not attending clubs; the boarding team hands devices out from, and collects them back into, the tech box.
- For all boarders, once Prep is completed, devices may be used in supervised communal areas only. Boarders have around one hour of tech time on weekday evenings and more at weekends.
- At bedtime boarders return their devices to the boarding team, who store them in the locked tech cupboard. Devices are not taken to dormitories. The same procedure applies at weekends.
- Boarders use the BOSBYOD network under adequate supervision, with devices set up by the IT team (see section 8.5).

12) COMMUNICATIONS: EMAIL, MESSAGING & SOCIAL MEDIA

12.1 Email and messaging

- The official school email service (Microsoft 365) is regarded as safe and secure and is monitored. Users should be aware that email communications are monitored.
- Users must immediately report to a teacher or the DSL any communication that makes them feel uncomfortable or is offensive, discriminatory, threatening or bullying in nature, and must not respond to it.
- Any digital communication between staff and pupils or parents must be professional in tone and content and only through official school systems (school email, Teams, iSAMS or approved platforms). Staff must not use personal accounts or personal messaging apps to contact pupils.
- Pupils must not reveal personal details of themselves or others in email communication or arrange to meet anyone without specific permission.
- Incoming email should be treated as suspicious and attachments or links not opened unless the sender is known and the message is expected. Suspected phishing is reported to the IT helpdesk.
- The forwarding of chain messages is not permitted.

12.2 Social media

- The school controls access to social media on its networks and educates pupils in its safe use, including privacy settings, passwords, nicknames and avatars, and never giving out details that could identify them or their location.
- Most social media platforms require users to be at least 13. Parents and pupils are advised of the risks of using social media outside school and of the minimum ages for each platform.

- Pupils must not post personal photos on any social space provided within school learning platforms.
- Staff must keep personal and professional profiles separate, must not accept pupils or recent former pupils as friends or followers on personal accounts, and must follow the Staff Code of Conduct.
- Official school social media accounts are managed by the Marketing team with the approval of the Headteacher, and follow the photograph consent register.
- Access to social media for boarders of an appropriate age is provided through the boarders' filter group during supervised tech time only.

13) USE OF DIGITAL & VIDEO IMAGES AND THE SCHOOL WEBSITE

13.1 Published content and the school website

- Contact details on the website are the school address, email and telephone number. Staff or pupils' personal information is not published.
- The Headteacher or nominee takes overall editorial responsibility and ensures that content is accurate and appropriate.

13.2 Publishing pupils' images and work

- Written permission from parents or carers is obtained when a pupil joins the school before photographs of pupils are published on the school website, social media or in the local press. Parents can change their consent at any time.
- Photographs that include pupils are selected carefully, and pupils' full names are not used alongside photographs.
- When using digital images, staff inform and educate pupils about the risks associated with taking, using, sharing, publishing and distributing images, including the risks of posting their own images online and of images being manipulated by AI.
- Further information can be found in our Privacy Notices and our Taking, Storing and Using Images of Pupils Policy.

13.3 Staff use of devices for photographs and video

Where photographs of pupils' activities are required (such as trips, celebrations, classroom practice, exemplar work and sport), staff should only take them on approved school devices or by using the ChatPro app on their own devices. ChatPro photos are not stored on the device, ChatPro logs all photos and who has viewed them, and only authorised staff may download them. Personal devices

must not be used in EYFS settings. Some pupils may feel sensitive or uncomfortable about having an image taken; staff should explain the purpose, respect a pupil's wishes and check the photo consent register before any publication or storage. Any photos downloaded must only be stored on school devices or secure school systems with permission from SLT. Staff must:

- store images securely so that they are used only by those authorised to do so;
- be clear about the purpose of the activity and what will happen to the images afterwards;
- ensure a senior member of staff is aware that photography is taking place and why;
- ensure all images are available to be screened for acceptability, and be able to justify any image made;
- not take photographs in one-to-one situations;
- be completely familiar with the register of parental consent. Taking, displaying or distributing images of pupils where there is no consent will be considered a breach of safeguarding duties.

14) DATA PROTECTION

Personal data is recorded, processed, transferred and made available in accordance with UK GDPR and the Data Protection Act 2018. Full details are in the Data Protection Policy.

The school ensures that:

- it has a Data Protection Policy and implements the data protection principles, and can demonstrate this through policies, notices and records;
- it has paid the appropriate fee to the Information Commissioner's Office (ICO) and has appointed a Data Protection Officer (DPO) with a high level of understanding of data protection law and no conflict of interest;
- it maintains an information asset register recording what personal data it holds, where, why, the lawful basis for processing (and, for special category data, the additional condition) and who is responsible for it;
- it holds only the minimum personal data necessary, keeps it accurate and up to date, and does not keep it longer than necessary, in line with its retention schedule;
- it provides clear Privacy Notices to staff, parents, pupils and volunteers, and has procedures to deal with individual rights, including subject access requests;
- Data Protection Impact Assessments (DPIAs) are carried out where necessary, for example for new systems, AI tools, remote access solutions or new suppliers, and data processing clauses are in place with all data processors;
- it shares data lawfully and safely with other relevant data controllers, remembering that data protection law does not prevent the sharing of information to keep children safe;

- it reports relevant breaches to the ICO within 72 hours of becoming aware of them, and to affected individuals where required, and has a procedure for reporting, logging, investigating and learning from information risk incidents;
- all staff receive data protection training at induction and regular refresher training thereafter.

When personal data is stored on any mobile device or removable media:

- the data must be encrypted and the device password protected;
- the device must be protected by up-to-date anti-virus and malware protection;
- the data must be securely deleted from the device once it has been transferred or its use is complete. Personal USB storage must not be used for school personal data.

Staff must:

- take care at all times to keep personal data safe, minimising the risk of its loss or misuse;
- recognise a possible breach, understand the urgency and report it immediately to the DPO and Head of IT;
- know how to recognise a subject access or other rights request (verbal or written) and who to pass it to;
- not transfer school personal data to personal devices or personal cloud or AI services, except as permitted by school policy;
- access personal data only on secure, password-protected devices and lock or log off at the end of every session.

15) MANAGING EMERGING TECHNOLOGIES & AUTHORISING ACCESS

15.1 Emerging technologies

Emerging technologies, including new apps, platforms, smart devices and AI tools, are examined for educational benefit. A risk assessment (and a DPIA where personal data is involved) is carried out by the Head of IT with the DSL before use in school is allowed, and approval is obtained at Globeducate group level. Filtering and monitoring are confirmed to work before release.

15.2 Authorising internet access

- All staff must read and sign the Staff IT Acceptable Use Policy / Code of Conduct before using any school IT resource.
- The school maintains a current record of all staff and pupils who are granted access to school IT systems, and removes access promptly when people leave.

- Pupils agree to the Pupil IT Rules when they join (through the parent joiner pack) and then annually in Computing lessons. Records are kept by the IT team.

- Visitors, contractors, lettings users and summer school staff agree to the Guest Acceptable Use Policy before using school internet access.
- Downloaded material, such as music files and images, must be appropriate, fit for purpose and used in accordance with copyright law.

15.3 Assessing risks

The school takes all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a school device. The school audits its technology use, using tools such as 360 degree safe, to establish whether this policy is adequate and is being implemented effectively.

16) RESPONDING TO ONLINE SAFETY INCIDENTS

All online safety incidents and concerns are reported to the DSL without delay and recorded as a serious incident on MyConcern (this replaces the former E-Safety incident form). The flowchart in Appendix 1 sets out the response.

16.1 Illegal incidents

If there is any suspicion that a website, device or message may contain child sexual abuse material, or if there is any other suspected illegal activity (such as grooming, sextortion or terrorist content), follow the right-hand side of the flowchart and report immediately to the DSL, who will contact the police. Staff must not investigate, view, copy or forward the material themselves; they should secure the device and preserve evidence.

16.2 Nudes and semi-nudes

Incidents involving the creation or sharing of nudes and semi-nudes by anyone under 18 – whether self-generated, created by another person, digitally altered or wholly AI-generated ("deepfakes" or "deep nudes"), and whether consensual or not – are handled by the DSL in line with the UKCIS guidance. Staff must never view, copy, print, share, save or ask a child to delete the image, or ask a child to send it to them. The DSL decides whether a referral to the police or Children's Services is needed. Children can be supported to use Childline and the IWF's Report Remove tool to get images removed.

16.3 Online sexual harassment, child-on-child abuse and bullying

Online sexual harassment and online bullying are forms of child-on-child abuse and are dealt with under the Child-on-Child Abuse and Anti-Bullying policies. Abuse can happen in and outside school, online and offline, and the school responds to reports regardless of where they took place.

16.4 Radicalisation and extremism

Concerns that a pupil may be at risk of radicalisation, or exposure to terrorist or extremist content, are reported to the DSL, who will consider a Prevent referral. Online terrorist content can also be reported to the police through the government's Report Terrorism service, and in an emergency by calling 999.

16.5 Concerns about staff

Any concern or allegation about a member of staff, volunteer or contractor's use of technology is referred to the Headteacher (or, if it concerns the Headteacher, to the Proprietor / Chair of the Advisory Board), who will follow the allegations management procedure and consult the LADO where appropriate. Low-level concerns are recorded in line with the Safeguarding Policy.

17) BEHAVIOUR, SANCTIONS & COMPLAINTS

17.1 Behaviour

Boundary Oak School will ensure that all users of technology adhere to the standards of behaviour set out in the Acceptable Use Policies. The school will not tolerate any abuse of IT systems. Whether offline or online, communications by staff and pupils should be courteous and respectful at all times. Any reported incident of bullying, harassment or other unacceptable conduct will be treated seriously and in line with the pupil and staff disciplinary codes. Where conduct is considered illegal, the school will report the matter to the police. This includes incidents of cyber-bullying, online sexual harassment and violence. Pupils should understand that making, possessing or sharing nude or semi-nude images of anyone under 18 is illegal, even if they are of themselves and even if they were shared consensually or are AI-generated, although the school's response will always put the welfare of the children involved first.

17.2 Sanctions

Staff and pupils are given information about infringements and sanctions. Sanctions may include:

- interview, counselling and/or disciplinary action by the teacher, Deputy Head or Headteacher;
- informing parents or carers;

- removal of internet, device or network access for a period;
- suspension or permanent exclusion, in line with the Behaviour Policy.

17.3 Handling complaints

- Complaints about internet misuse by pupils are dealt with in the first instance by the DSL, with technical support from the Head of IT.
- Any complaint about staff misuse is referred to the Headteacher and may result in formal disciplinary proceedings.
- Complaints of cyber-bullying are dealt with in accordance with the Anti-Bullying Policy, and complaints related to child protection in accordance with the Safeguarding Policy.
- Pupils and parents are informed of the complaints procedure and of the consequences of misusing the internet.

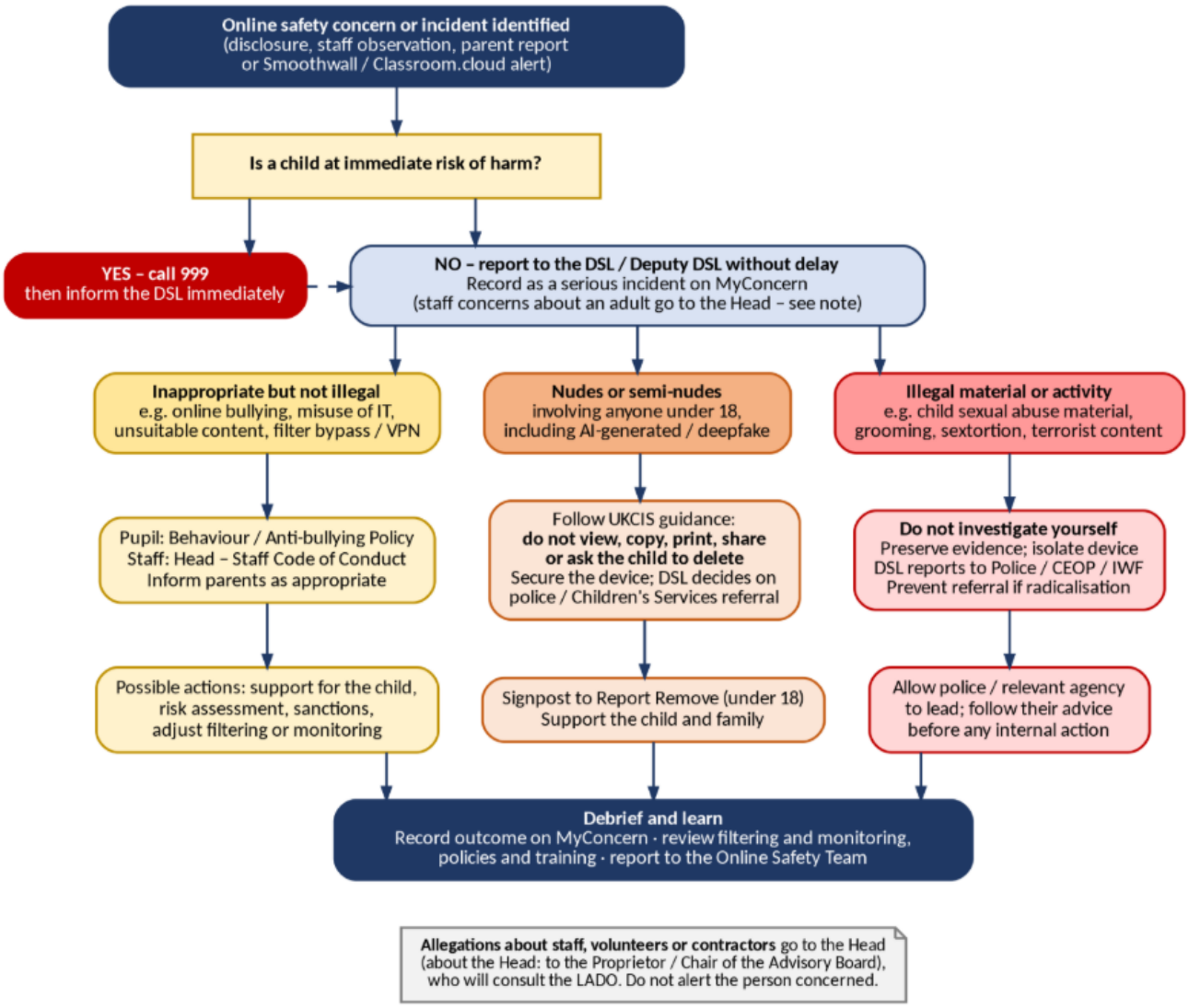
18) MONITORING, REVIEW & IMPACT

The impact of this policy is monitored regularly by the Online Safety Team through incident records on MyConcern, filtering and monitoring reports and checks, pupil and parent feedback and staff training records. The policy is fully reviewed at least annually by the SLT and approved by the Advisory Board, alongside the annual filtering and monitoring review. If concerns are raised in the interim – triggered by incidents, changes to statutory guidance or technology, or unforeseen circumstances – the review will be brought forward.

19) APPENDICES

Appendix 1 – Online Safety Incident Flowchart

Record every incident as a serious incident on MyConcern. If in doubt, speak to the DSL. If a child is at immediate risk, call 999.



Appendix 2 – Filtering and Monitoring Check Log & Annual Review Record

KCSIE 2026 requires the school to keep a record of filtering checks and to be able to demonstrate that the annual review of filtering and monitoring has taken place. This template is kept on the Online Safety SharePoint.

A – REGULAR (MONTHLY) CHECK LOG

Date	Checked By	Device/Location/UserGroup	What was tested?	Result	Action taken (by whom and by when)
		e.g. pupil Chromebook, Year 5 classroom, pupil account	SWGfL Test Filtering; blocked categories; AI tool filtering; Smoothwall alert received	Pass/Fail	
		e.g. boarder phone on BOSBYOD after 5.30pm			
		e.g. staff laptop off site			
		e.g. guest Wi-Fi, visitor device			

B – ANNUAL REVIEW RECORD

Item	Record
Date of review	
Led by (SLT lead for filtering and monitoring)	
Supported by (DSL / Head of IT / provider)	
Risk profile considered (age range, SEND, boarding, EAL, BYOD, AI use, recent incidents)	
Filtering and monitoring providers and what they block / alert on	
Devices, locations and user groups tested	
Gaps against the DfE filtering and monitoring standards	
Actions agreed (owner and deadline)	
Reported to the Proprietor / Advisory Board on	

Appendix 3 – UK Online Safety Portals, Helplines and Reporting

All links below are UK services. In an emergency, or if a child is in immediate danger, call 999. For non-emergency police matters call 101. Concerns about a child at Boundary Oak should always be shared with the DSL as well.

A – FOR STAFF

Service	What it Offers	Link
Keeping Children Safe in Education 2026	Statutory safeguarding guidance; all staff read Part One and Annex A	gov.uk – KCSIE
DfE Filtering and Monitoring Standards	The standards used for our checks and annual review	gov.uk – filtering standards
DfE Cyber Security Standards	Cyber security expectations for schools	gov.uk – cyber standards
Generative AI product safety expectations	DfE expectations for AI tools used in education	gov.uk – generative AI
UKCIS – Sharing nudes and semi-nudes	How to respond to incidents involving nudes and semi-nudes	gov.uk – UKCIS advice
Professionals Online Safety Helpline (UK Safer Internet Centre)	Free advice for anyone working with children on any online safety issue, including getting content removed	swgfl.org.uk – POSH
UK Safer Internet Centre	Guidance on appropriate filtering and monitoring, Safer Internet Day resources	saferinternet.org.uk
SWGfL Test Filtering / 360 degree safe	Check our filtering; online safety self-review tool	swgfl.org.uk – Test Filtering swgfl.org.uk – 360 degree safe
ProjectEVOLVE	Curriculum resources mapped to Education for a Connected World	swgfl.org.uk – ProjectEVOLVE
CEOP Education (National Crime Agency)	Lesson plans and training on online sexual abuse	ceopeducation.co.uk/professionals
NSPCC Learning	Safeguarding training, CASPAR briefings and online safety research	learning.nspcc.org.uk
Childnet – Teachers and professionals	PSHE toolkits and classroom resources	childnet.com
Educate Against Hate / ACT Early	Prevent resources; advice on radicalisation concerns	educateagainsthate.com actearly.uk
NCSC – Cyber security for schools	Free staff cyber training and guidance	ncsc.gov.uk – schools
Information Commissioner's Office	Data protection guidance; reporting a personal data breach	ico.org.uk – report a breach
Hampshire Safeguarding Children Partnership	Local safeguarding procedures, LADO and referral information	hampshirescp.org.uk
Revenge Porn Helpline / StopNCII	Support for adults (18+), including staff, affected by intimate image abuse	revengepornhelpline.org.uk stopncii.org
National College	Staff online safety and safeguarding CPD (school subscription)	nationalcollege.com

B – FOR PUPILS

Service	What it Offers	Link
Childline	Free, confidential help for anyone under 19, by phone (0800 1111), online chat or email	childline.org.uk
Report Remove (Childline and IWF)	Helps under-18s get nude images or videos of themselves removed from the internet	childline.org.uk – Report Remove
CEOP Safety Centre	Report online sexual abuse or someone who is making you feel uncomfortable	ceop.police.uk
CEOP Education	Age-appropriate advice for young people (formerly Thinkuknow)	ceopeducation.co.uk
Childnet – Young people	Tips and help on staying safe online	childnet.com/young-people
Report Harmful Content	Help reporting harmful content such as bullying, threats or impersonation	reportharmfulcontent.com
Take It Down	Helps remove nude images of under-18s from participating platforms	takeitdown.ncmec.org
Shout	Free 24/7 text support: text SHOUT to 85258	giveusashout.org
The Mix	Support for 13–25-year-olds on any issue	themix.org.uk
In school	Talk to any trusted adult, or use the "Report suspicious activity online" button on the pupil Useful Links page	

C – FOR PARENTS AND CARERS

Service	What it Offers	Link
Boundary Oak E-Safety website	Our school guidance, this policy and forms	Boundary Oak E-Safety site
Internet Matters	Step-by-step parental control guides for devices, consoles, broadband and apps; age-by-age advice	internetmatters.org
NSPCC – Online safety	Advice on apps, games and talking to your child; NSPCC Helpline 0808 800 5000	nspcc.org.uk – online safety
CEOP Education – Parents and carers	Advice and activities to use at home	ceopeducation.co.uk/parents
UK Safer Internet Centre – Parents	Guides, conversation starters and reporting help	saferinternet.org.uk – parents
Childnet – Parents and carers	Family agreements and topic guides	childnet.com/parents-and-carers
Parent Zone	Advice on digital family life, gaming and scams	parentzone.org.uk
PEGI	Age ratings and content descriptors for games	pegi.info
Report Harmful Content	Help reporting harmful content online	reportharmfulcontent.com
Action Fraud	Report fraud, scams and cyber crime	actionfraud.police.uk

D – REPORTING ILLEGAL OR HARMFUL CONTENT

Service	What it Offers	Link
Child sexual abuse images or videos online	Internet Watch Foundation (anonymous)	report.iwf.org.uk
Online grooming or sexual abuse of a child	CEOP (National Crime Agency) – and 999 in an emergency	ceop.police.uk
Terrorist or extremist content	Report Terrorism (Counter Terrorism Policing)	gov.uk/report-terrorism
Phishing emails and texts	NCSC – forward emails to report@phishing.gov.uk; texts to 7726; Anti-Phishing Working Group	apwg.org
Fraud and cyber crime	Action Fraud	actionfraud.police.uk
Personal data breach (school)	DPO and Head of IT immediately; ICO within 72 hours where required	ico.org.uk

Appendix 4 – Guidance for Parents & Carers

"Wherever your child goes online, so should you." Children range from the most vulnerable to the most resilient; understanding where your child sits on the spectrum of vulnerability is the first step to knowing the level of protection they need. These are guidelines to use as appropriate for your child's age and maturity.

GET INVOLVED

- Know which devices, apps and games your child uses, and whether they allow chat or contact with strangers. Ask your child to show you how they play and who they interact with.
- Be aware of the minimum age for each platform (most social media is 13+) and of game age ratings (PEGI). See the school E-Safety site and Internet Matters.
- Talk regularly and calmly, and ask your child why they think you might worry about the internet – check they understand the hidden risks.
- Agree family rules together: when and where devices can be used, how long for, and what sites, games and apps are allowed. Keep devices out of bedrooms overnight.
- Be alert to signs of radicalisation, sextortion, gambling and unhealthy attachment to AI chatbots, and to the indicators of risk in section 3 of this policy.

SET UP CONTROLS

- Turn on your broadband provider's free family filters, and use the parental controls built into devices and consoles (for example Apple Screen Time, Google Family Link, Microsoft Family Safety, Xbox, PlayStation and Nintendo family settings).
- Set up your child's accounts yourself where possible, keep a record of passwords, set profiles to private, turn off location sharing and restrict who can contact them.
- Restrict in-app purchases and do not leave payment cards stored on devices or accounts your child uses.
- Remember that filters and controls are not foolproof – they work best alongside conversation and supervision.

What should not be on a child's profile

Full name, date of birth, address, school, mobile number, email address, photos in school uniform, routines, holiday countdowns, location check-ins, relationship status, or details of what they are scared of. This information can help someone identify and locate a child or build a false sense of trust. Children who share personal characteristics online can also be targeted for bullying, so talk with your child about what they share and who can see it. *(Source: University of Bedfordshire)*

If something goes wrong

- Stay calm, listen and reassure your child that they are not in trouble for telling you.
- Save evidence of bullying or threats (screenshots of messages and profiles) – but never screenshot, copy, forward or save a nude or semi-nude image of a child, even to report it.
- If your child is being threatened or blackmailed over images, do not pay or engage; block and report the account, contact the police (and CEOP), and use Report Remove.
- Let the school know if other pupils are involved, so that the DSL can help.
- Do not allow online abuse to distract you from the very real, and still more common, risk of abuse by people a child already knows.

Talk to children about peer pressure

We help children to resist pressure to: meet someone they have only met online; get into a car or a taxi with someone they don't know; go alone to a house they don't know; accept drinks or gifts from someone they have just met; give their mobile number or social media details to strangers; or do anything physical or sexual they are not comfortable with.

Appendix 5 – Apps, Platforms & Features to be Aware of

Apps change quickly, so this appendix focuses on the **features** that create risk rather than a fixed list of apps. For up-to-date reviews of individual apps and games, see Internet Matters and the NSPCC online safety pages (Appendix 3). Omegle, which featured in previous versions of this policy, closed in 2023, but similar random video-chat sites continue to appear.

Feature	Examples	Why it Matters
Random or anonymous chat	Random video-chat sites; anonymous Q&A and messaging apps	Contact with strangers, sexual content, and anonymous bullying.
Disappearing messages and "stories"	Snapchat, Instagram, WhatsApp view-once	A false sense that images vanish – they can be screenshotted and shared.
Location sharing	Snap Map, Find My, family-tracking apps, check-ins	Can reveal a child's home, school and routine to others.
Livestreaming and gifting	TikTok LIVE, YouTube, Twitch	Real-time contact with strangers; requests for gifts or acts on camera.
Gaming with open chat and voice	Roblox, Fortnite, Minecraft servers, Discord	Grooming via "help" in the game or gifts of in-game currency; abusive language over headsets; moving the chat to another app.
Large or encrypted group chats	WhatsApp, Telegram, Signal, Discord servers	Children added to groups by strangers; harmful or extreme content spread quickly; few parental controls.
AI chatbots and companions	General AI assistants, AI "friend" and character apps	Emotional dependence, sexualised or harmful conversations, inaccurate advice.
Image manipulation / "nudify" tools	Face-swap, deepfake and nudify apps and websites	Creation of AI-generated nudes of real people – illegal where the person is under 18.
Gambling-like features	Loot boxes, skin betting, in-game purchases	Normalises gambling; unexpected spending.
"Chain" or "proud parent" posts	Social media challenges asking parents to share photos of their children	Images of children harvested and misused.

Appendix 6 – Glossary of Terms and Acronyms

Term/Acronym	Meaning
360 degree safe	SWGfL's online safety self-review tool for schools.
Age-related filtering	Differentiated access to online content managed by the school according to age and need (BOS uses Smoothwall).
AI / GenAI	Artificial intelligence / generative AI – tools that create text, images, audio or video (e.g. chatbots, image generators).
AI companion	An AI chatbot designed to simulate friendship or a relationship.
APWG	Anti-Phishing Working Group – international body to which phishing can be reported (referenced in KCSIE 2026).
AUP	Acceptable Use Policy.
BYOD	Bring Your Own Device – pupils' own devices connected to the BOSBYOD network.
CA certificate	Security certificate installed on BYOD devices so that encrypted web traffic can be filtered and monitored.
CCE / CSE	Child Criminal Exploitation / Child Sexual Exploitation.
CEOP	Child Exploitation and Online Protection Command of the National Crime Agency.
CSAM	Child Sexual Abuse Material (illegal images or videos of children).
Cyber-bullying	Bullying using technology such as phones, social media, games or messaging.
Deepfake / deep nude	Image, video or audio digitally altered or generated by AI to show a real person doing or saying something they did not; a "deep nude" is a sexualised deepfake.
DfE	Department for Education.
Disinformation / misinformation	False information spread deliberately to deceive (disinformation) or shared without knowing it is false (misinformation).
DPIA	Data Protection Impact Assessment.
DPO	Data Protection Officer.
DSL / DDSL	Designated Safeguarding Lead / Deputy Designated Safeguarding Lead.
EYFS	Early Years Foundation Stage.
Encryption	Scrambling data so it cannot be read without a key, protecting it if a device is lost or stolen.
Filtering	Technology that blocks access to harmful or inappropriate online content.
Grooming	Building a relationship, trust and emotional connection with a child in order to manipulate, exploit and abuse them.
Hacker	A person who gains unauthorised access to computer systems or accounts.
HSB	Harmful Sexual Behaviour.
ICO	Information Commissioner's Office – the UK data protection regulator.
IIA / NCII	Intimate Image Abuse / Non-Consensual Intimate Imagery.
ISI	Independent Schools Inspectorate.
IWF	Internet Watch Foundation – removes child sexual abuse imagery online.
KCSIE	Keeping Children Safe in Education – statutory safeguarding guidance for schools in England.

LADO	Local Authority Designated Officer – manages allegations against adults who work with children.
MFA	Multi-Factor Authentication.
Monitoring	Technology and supervision that identify concerning online activity so that staff can respond.
NCA	National Crime Agency.
NCSC	National Cyber Security Centre.
Nudes and semi-nudes	KCSIE 2026 term for nude or semi-nude images or videos of under-18s, whether self-generated, created by others, altered or AI-generated.
OSA	Online Safety Act 2023 – places duties on online platforms, regulated by Ofcom.
Phishing	Fraudulent messages designed to steal passwords, money or personal information.
POSH	Professionals Online Safety Helpline (UK Safer Internet Centre).
Prevent	The government's strategy to stop people being drawn into terrorism.
PSHE / RSHE	Personal, Social, Health and Economic education / Relationships, Sex and Health Education.
Sextortion	Blackmail using sexual images, often financially motivated.
SLT / SMT	Senior Leadership Team / Senior Management Team.
SWGfL	South West Grid for Learning – online safety charity and partner in the UK Safer Internet Centre.
UK GDPR / DPA 2018	UK General Data Protection Regulation and the Data Protection Act 2018.
UKCIS	UK Council for Internet Safety.
UKSIC	UK Safer Internet Centre.
VPN / proxy	Tools that hide or reroute internet traffic and can be used to bypass school filtering; not permitted on school networks.
WTSC	Working Together to Safeguard Children (statutory guidance).

TEXT AND INTERNET CODES

Young people use shorthand to send messages quickly, sometimes so that supervising adults don't understand them. Slang changes constantly, so treat this list as illustrative and check current guides such as Internet Matters.

Term/Acronym	Meaning
LMIRL	Let's meet in real life
IWSN	I want sex now
8	Oral sex
IMEZRU	I am easy, are you?
TDTM	Talk dirty to me
CU46	See you for sex
MPFB	My personal f**k buddy
SORG	Straight or gay?
WYFM	Would you f**k me?

420	Marijuana
XTC	Ecstasy
MOOS	Member of the opposite sex
AITR	Adult in the room
MOS / POS	Mum / parent over shoulder
PIR	Parent in room
CD9 / Code 9	Parents are nearby
KPC	Keeping parents clueless
P911	Parent alert
PAL / PAW	Parents are listening / watching
ASLP	Age, sex, location, picture
A3	Anytime, any place, anywhere
COBRAS	Come on by right after school
9 / 99	Parent watching / parent no longer watching
NP	Nosy parents or no problem
121	One to one
143	I love you
53X	Sex