Online Safety Policy	
Updated	October 2026
Status	Non-Statutory policy
Review	October 2027

Statement of intent

Compass School understands that using online services is an important aspect of raising educational standards, promoting pupil achievement, and enhancing teaching and learning. The use of online services is embedded throughout the school; therefore, there are a number of controls in place to ensure the safety of pupils and staff.

The breadth of issues classified within online safety is considerable, but they can be categorised into four areas of risk:

- Content: Being exposed to illegal, inappropriate or harmful material, e.g., pornography, racism, misogyny, self-harm and suicide, radicalisation, extremism, extreme sexual or physical violence, misinformation, disinformation and conspiracy theories.
- Contact: Being subjected to harmful online interaction with other users or generative AI applications that simulate harmful interaction, e.g., peer pressure, commercial advertising, and adults posing as children or young adults with the intention to groom or exploit children for sexual, criminal, financial or other purposes.
- Conduct: Online behaviour that increases the likelihood of, or causes, harm, e.g., making, sending and receiving explicit images, including self-generated intimate images and/or videos and content generated or altered using AI (including deepfakes), and online bullying.
- Commerce: Risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

Conduct: Online behaviour that increases the likelihood of, or causes, harm, e.g., making, sending and receiving explicit images, including self-generated intimate images and/or videos and content generated or altered using AI (including deepfakes), and online bullying.

1. Legal framework

This policy has due regard to all relevant legislation and guidance including, but not limited to, the following:

• Voyeurism (Offences) Act 2019
• UK General Data Protection Regulation (UK GDPR)
• Data Protection Act 2018
• Data (Use and Access) Act 2025
• Children's Wellbeing and Schools Act 2026
• DfE (2026) Keeping children safe in education (KCSIE), in force from 1 September 2026
• DfE (2026) Mobile phones in schools
• DfE (2026) Meeting digital and technology standards in schools and colleges – Filtering and monitoring: core standard
• DfE (2021) Harmful online challenges and online hoaxes
• DfE (2023) Teaching online safety in schools
• DfE (2022) Searching, screening and confiscation
• DfE (2026) Generative AI: product safety standards
• DfE (2025) Generative artificial intelligence in education
• DfE (2025) Relationships Education, Relationships and Sex Education (RSE) and Health Education – revised guidance for introduction 1 September 2026
• UKCIS / DSIT (2024) Sharing nudes and semi-nudes: advice for education settings working with children and young people
• UKCIS (2020) Education for a Connected World – 2020 edition
• National Cyber Security Centre – Cyber security standards for schools and colleges

The headteacher will be responsible for:

- Ensuring that online safety is a running and interrelated theme throughout the school's policies and procedures, including in those related to the curriculum, teacher training and safeguarding.
- Supporting the DSL and the deputy DSL by ensuring they have enough time and resources to carry out their responsibilities in relation to online safety.
- Ensuring staff receive regular, up-to-date and appropriate online safety training and information as part of their induction and safeguarding training.
- Ensuring online safety practices are audited and evaluated.

The DSL and DDSL will be responsible for:

- Taking the lead responsibility for online safety in the school.
- Undertaking training so they understand the risks associated with online safety
- Liaising with relevant members of staff on online safety matters.
- Ensuring online safety is recognised as part of the school's safeguarding responsibilities and that a coordinated approach is implemented.
- Establishing a procedure for reporting online safety incidents and inappropriate internet use, both by pupils and staff, and ensuring all members of the school community understand this procedure.
- Understanding the filtering and monitoring processes in place at the school.
- Organising engagement with parents to keep them up to date with current online safety issues and how the school is keeping pupils safe.
- Ensuring that all safeguarding training given to staff includes an understanding of the expectations, roles and responsibilities in relation to filtering and monitoring systems at the school.
- Maintaining detailed, secure and accurate written records of reported online safety concerns as well as the decisions and whether or not referrals have been made.
- Understanding the purpose of record keeping.
- Monitoring online safety incidents to identify trends and any gaps in the school's provision and using this data to update the school's procedures.
- Reporting to the Management Committee about online safety on a termly basis.

Network technicians will be responsible for:

- Providing technical support in the development and implementation of the school's online safety policies and procedures.
- Implementing appropriate security measures as directed by the headteacher.
- Ensuring that the school's filtering and monitoring systems are updated as appropriate.

All staff members will be responsible for:

- Taking responsibility for the security of ICT systems and electronic data they use or have access to.
- Modelling good online behaviours.
- Maintaining a professional level of conduct in their personal use of technology.
- Having an awareness of online safety issues.
- Ensuring they are familiar with, and understand, the indicators that pupils may be unsafe online.
- Reporting concerns in line with the school's reporting procedure.
- Where relevant to their role, ensuring online safety is embedded in their teaching of the curriculum.

2. Managing online safety

All staff will be aware that technology is a significant component in many safeguarding and wellbeing issues affecting young people, particularly owing to the rise of social media and the increased prevalence of children using the internet.

The headteacher has overall responsibility for the school's approach to online safety, with support from DDSL where appropriate, and will ensure that there are strong processes in place to handle any concerns about pupils' safety online. A DSLO should liaise with the police or children's social care services for support responding to harmful online sexual behaviour.

The importance of online safety is integrated across all school operations in the following ways:

- Staff and the Management Committee receive regular training
- Staff receive regular email updates regarding online safety information and any changes to online safety guidance or legislation
- Online safety is integrated into learning throughout the curriculum
- School website page is regularly updated

Handling online safety concerns

Any disclosures made by pupils to staff members about online abuse, harassment or exploitation, whether they are the victim or disclosing on behalf of another child, will be handled in line with the Child Protection and Safeguarding Policy.

Staff will be aware that harmful online sexual behaviour can progress on a continuum, and appropriate and early intervention can prevent abusive behaviour in the future. Staff will also acknowledge that pupils displaying this type of behaviour are often victims of abuse themselves and should be suitably supported.

The victim of online harmful sexual behaviour may ask for no one to be told about the abuse. The DSL will consider whether sharing details of the abuse would put the victim in a more harmful position, or whether it is necessary in order to protect them from further harm. Ultimately the DSL will balance the victim's wishes against their duty to protect the victim and other young people. The DSL and other appropriate staff members will meet with the victim's parents to discuss the safeguarding measures that are being put in place to support their child and how the report will progress.

Confidentiality will not be promised, and information may be still shared lawfully, for example, if the DSL decides that there is a legal basis under UK GDPR such as the public task basis whereby it is in the public interest to share the information. If the decision is made to report abuse to children's social care or the police against the victim's wishes, this must be handled extremely carefully – the reasons for sharing the information should be explained to the victim and appropriate specialised support should be offered.

Concerns regarding a staff member's online behaviour are reported to the headteacher, who decides on the best course of action in line with the relevant policies. If the concern is about the headteacher, it is reported to the chair of Management Committee

Where there is a concern that illegal activity has taken place, the headteacher contacts the police.

The school avoids unnecessarily criminalising pupils, e.g., calling the police, where criminal behaviour is thought to be inadvertent and because of ignorance or normal developmental curiosity, e.g., a pupil has taken and distributed indecent imagery of themselves. The DSL will decide in which cases this response is appropriate and will manage such cases in line with the Child Protection and Safeguarding Policy.

3. Cyberbullying

Cyberbullying can include, but is not limited to, the following:

- Threatening, intimidating or upsetting text messages
- Threatening or embarrassing pictures and video clips sent via mobile phone cameras
- Silent or abusive phone calls or using the victim's phone to harass others, to make them think the victim is responsible
- Threatening or bullying emails, possibly sent using a pseudonym or someone else's name
- Unpleasant messages sent via instant messaging
- Unpleasant or defamatory information posted to blogs, personal websites and social networking sites, e.g., Facebook
- Abuse between young people in intimate relationships online i.e., teenage relationship abuse
- Discriminatory bullying online i.e., homophobia, racism, misogyny/misandry.

Cyberbullying against pupils or staff is not tolerated under any circumstances.

4. Child-on-child abuse (including harassment and violence)

All staff will be aware of the indicators of abuse, neglect and exploitation and understand where the risk of such harms can occur online. Staff will understand that child-on-child abuse can occur both in and outside of school, off and online, and that pupils may be less likely to report concerning online behaviour.

Staff will be alert to harmful online sexual behaviour, including sexual harassment, sexual violence, coercive or controlling behaviour, misogynistic or misandrist messages, the non-consensual sharing of self-generated intimate images and/or videos, including those generated or altered using AI (e.g. deepfakes), and the sharing of abusive images or pornography with people who do not want to receive such content.

- The school will maintain a zero-tolerance approach to sexually harassing or abusive behaviour and will not dismiss such behaviour as 'banter', 'just having a laugh' or harmless. Staff will understand that allowing such behaviour to continue can normalise abuse and discourage reporting.
- The school will respond to all concerns regarding online child-on-child abuse, regardless of whether the incident took place on school premises, outside school or using school-owned or personal equipment. Concerns will be reported to the DSL/DDSL and managed in line with the Child Protection and Safeguarding Policy.
- Where nudes or semi-nudes involving children are reported, the school will follow the Child Protection and Safeguarding Policy and relevant DfE/UKCIS guidance. Staff will not promise confidentiality and will ensure that the child is supported and not unnecessarily criminalised.

5. Grooming and exploitation

Grooming is defined as the situation whereby an adult builds a relationship, trust and emotional connection with a child with the intention of manipulating, exploiting and/or abusing them.

Staff will be aware that grooming often takes place online and that pupils who are being groomed are commonly unlikely to report this behaviour for many reasons, e.g., the pupil may have been manipulated into feeling a strong bond with their groomer and may have feelings of loyalty, admiration, or love, as well as fear, distress and confusion.

Due to the fact pupils are less likely to report grooming than other online offences, it is particularly important that staff understand the indicators of this type of abuse. The DSL and DDSL will ensure that online safety training covers online abuse, the importance of looking for signs of grooming, and what the signs of online grooming are, including:

- Being secretive about how they are spending their time online.
- Having an older boyfriend or girlfriend, usually one that does not attend the school and whom their close friends have not met.
- Having money or new possessions, e.g., clothes and technological devices, that they cannot or will not explain.

Child sexual exploitation (CSE) and child criminal exploitation (CCE)

Although CSE often involves physical sexual abuse or violence, online elements may be prevalent, e.g., sexual coercion and encouraging children to behave in sexually inappropriate ways through the internet. In some cases, a pupil may be groomed online to become involved in a wider network of exploitation, e.g., the production of child pornography or forced child prostitution and sexual trafficking.

CCE is a form of exploitation in which children are forced or manipulated into committing crimes for the benefit of their abuser, e.g., drug transporting, shoplifting and serious violence. While these crimes often take place in person, it is increasingly common for children to be groomed and manipulated into participating through the internet.

Where staff have any concerns about pupils with relation to CSE or CCE, they will bring these concerns to the DSL without delay, who will manage the situation in line with the Child Protection and Safeguarding Policy.

Radicalisation

Radicalisation is the process by which a person comes to support terrorism and extremist ideologies associated with terrorist groups. This process can occur through direct recruitment, e.g., individuals in extremist groups identifying, targeting and contacting young people with the intention of involving them in terrorist activity, or by exposure to violent ideological propaganda. Children who are targets for radicalisation are likely to be groomed by extremists online to the extent that they believe the extremist has their best interests at heart, making them more likely to adopt the same radical ideology.

Staff members will be aware of the factors which can place certain pupils at increased vulnerability to radicalisation, as outlined in the Prevent Policy. Staff will be expected to exercise vigilance towards any pupils displaying indicators that they have been, or are being, radicalised.

Where staff have a concern about a pupil relating to radicalisation, they will report this to the DSL without delay, who will handle the situation in line with the Prevent Policy.

6. Mental health

Staff will be aware that online activity both in and outside of school can have a substantial impact on a pupil's mental state, both positively and negatively. The DSL and DDSL will ensure that training is available to help ensure that staff members understand popular social media sites and terminology, the ways in which social media and the internet in general can impact mental health, and the indicators that a pupil is suffering from challenges in their mental health.

7. Online hoaxes and harmful online challenges

For the purposes of this policy, an **"online hoax"** is defined as a deliberate lie designed to seem truthful, normally one that is intended to scaremonger or to distress individuals who come across it, spread on online social media platforms.

For the purposes of this policy, **"harmful online challenges"** refers to challenges that are targeted at young people and generally involve users recording themselves participating in an online challenge, distributing the video through social media channels and daring others to do the same. Although many online challenges are harmless, an online challenge becomes harmful when it could potentially put the participant at risk of harm, either directly as a result of partaking in the challenge itself or indirectly as a result of the distribution of the video online – the latter will usually depend on the age of the pupil and the way in which they are depicted in the video.

Where staff suspect there may be a harmful online challenge or online hoax circulating amongst pupils in the school, they will report this to the DSL immediately.

The headteacher will conduct a case-by-case assessment for any harmful online content brought to their attention, establishing the scale and nature of the possible risk to pupils, and whether the risk is one that is localised to the school or the local area, or whether it extends more widely across the country. Where the harmful content is prevalent mainly in the local area, the headteacher will consult with the LA about whether quick local action can prevent the hoax or challenge from spreading more widely.

Prior to deciding how to respond to a harmful online challenge or hoax, the headteacher will decide whether each proposed response is:

- In line with any advice received from a known, reliable source, e.g., the UK Safer Internet Centre, when fact-checking the risk of online challenges or hoaxes.
- Careful to avoid needlessly scaring or distressing pupils.
- Not inadvertently encouraging pupils to view the hoax or challenge where they would not have otherwise come across it, e.g., where content is explained to younger pupils but is almost exclusively being shared amongst older pupils.
- Proportional to the actual or perceived risk.
- Helpful to the pupils who are, or are perceived to be, at risk.
- Appropriate for the relevant pupils' age and developmental stage.
- Supportive
- In line with the Child Protection and Safeguarding Policy.

Where the headteacher's assessment finds an online challenge to be putting pupils at risk of harm, they will ensure that the challenge is directly addressed to the relevant pupils, e.g., those within a particular age range that is directly affected or individual pupils at risk where appropriate.

The headteacher will only implement a school-wide approach to highlighting potential harms of a hoax or challenge when the risk of needlessly increasing pupils' exposure to the risk is considered and mitigated as far as possible.

8. Cyber-crime

Cyber-crime is criminal activity committed using computers and/or the internet. There are two key categories of cyber-crime:

- **Cyber-enabled** – these crimes can be carried out offline; however, are made easier and can be conducted at higher scales and speeds online, e.g., fraud, purchasing and selling of illegal drugs, and sexual abuse and exploitation.
- **Cyber-dependent** – these crimes can only be carried out online or by using a computer, e.g., making, supplying or obtaining malware, illegal hacking, and 'booting', which means overwhelming a network, computer or website with internet traffic to render it unavailable.

The school will factor into its approach to online safety the risk that pupils with a particular affinity or skill in technology may become involved, whether deliberately or inadvertently, in cyber-crime.

The headteacher will ensure that pupils are taught, throughout the curriculum, how to use technology safely, responsibly and lawfully.

The school is committed to robust cyber awareness for pupils and staff to ensure that they understand the basics of cyber security and protecting themselves from cybercrime.

The school will implement its cyber security strategy in line with the DfE's 'Cyber security standards for schools and colleges and the Cyber Security Policy.

9. Online safety training for staff

Training will include recognition of AI-generated or digitally altered harmful imagery, deepfakes, online grooming and exploitation, harmful online communities, misogynistic or violent online content, cybercrime, misinformation and disinformation, and routes for reporting concerns.

All staff will understand that pupils are at risk of abuse and other harms by peers and adults online as well as in person, and that harm may take place concurrently through online and offline channels.

All staff will be required to complete the school's annual safeguarding/online safety training and relevant updates during the year.

The DSL and DDSL will ensure that all safeguarding training given to staff includes online safety, including how the internet and digital technologies can facilitate abuse and exploitation, emerging AI-related safeguarding risks, and the expectations, roles and responsibilities relating to filtering and monitoring systems.

10. Online safety and the curriculum

Online safety is embedded throughout the curriculum in all subjects and is particularly addressed through Relationships, Sex and Health Education, Social, Physical, Intellectual, Creative and Emotional education, Personal, Social, Health and Economic Education, and Computing.

- The school will implement the revised Relationships Education, RSE and Health Education statutory guidance from 1 September 2026, including age- and stage-appropriate teaching about online harms.
- Pupils will be taught about online harms including sharing images, the prevalence and harms of deepfakes, pornography, misogynistic and violent online content, misinformation and disinformation, and when and where to seek help.
- Pupils will be taught the underpinning knowledge and behaviours that enable them to navigate the online world safely and confidently, regardless of the device, platform or app they use. This includes evaluating online information, recognising persuasion and manipulation, understanding acceptable and unacceptable behaviour, identifying risks, protecting personal information, understanding the consequences of sharing material, and knowing how and when to seek support.

Teaching will be age- and developmentally appropriate and will take account of pupils with SEND and other vulnerabilities. The curriculum will be reviewed in response to emerging risks and relevant incidents.

The DSL will be involved in the development of the online safety curriculum. Pupils will be consulted where appropriate because of their knowledge of the websites, platforms and behaviours used by them and their peers.

Class teachers will review external resources before use. External visitors will be appropriately checked and selected by the headteacher.

Any safeguarding concern or disclosure arising from online safety teaching will be reported in line with the Child Protection and Safeguarding Policy.

11. Use of technology in the classroom

A wide range of technology will be used during lessons, including the following:

- Computers
- Laptops
- Tablets
- Intranet
- Email
- Cameras

Prior to using any websites, tools, apps or other online platforms in the classroom, or recommending that pupils use these platforms at home, the class teacher will review and evaluate the resource. Class teachers will ensure that any internet-derived materials are used in line with copyright law.

Pupils will be supervised when using online materials during lesson time – this supervision is suitable to their age and ability.

12. Use of smart technology and mobile phones

The school recognises that smart technology can have educational benefits but also presents safeguarding, behaviour and wellbeing risks.

The school will operate as a mobile phone-free environment by default, in accordance with the DfE statutory guidance 'Mobile phones in schools'. The school's Behaviour Policy/mobile phone arrangements will set out the practical rules, exceptions, reasonable adjustments and consequences for non-compliance.

The prohibition applies throughout the school day, including lessons, the time between lessons, breaktimes and lunchtime, unless an agreed exception applies.

- The same approach will apply to other smart technology with similar functionality where the school determines that it presents equivalent risks.
- Pupils will be taught about the risks associated with mobile phones and smart technology, including distraction, bullying, harmful content, image-sharing and privacy risks.
- Inappropriate use may include sexual harassment, bullying, trolling or intimidation; sharing nudes or semi-nudes, including AI-generated or altered imagery; viewing or sharing pornography or other harmful content; and recording or distributing material without consent.

Staff will use smart technology and personal devices in line with the Staff ICT Policy and Staff Code of Conduct.

The school will keep its arrangements under review as devices, platforms, apps, AI tools and associated threats develop.

The school will consider the 4Cs (content, contact, conduct and commerce) when educating pupils about online risk and when responding to incidents.

13. Use of AI

As AI tools become increasingly common in education and the workplace, the school recognises that they are a valuable tool for saving time, generating ideas and supporting teaching and administration. However, they must always be used safely, responsibly and with professional judgement.

Pupils are not allowed access to AI platforms at all in school and staff have been issued with guidance on how to use AI safely

The final responsibility for anything produced using AI remains with the member of staff using it.

AI can be used for:

- Generating ideas for lessons, activities, starters, quizzes and revision tasks
- Creating lesson plans and teaching resources
- Adapting resources for different levels or abilities
- Generating examples, questions, scenarios or explanations to support teaching
- Helping to draft routine communications, such as letters or general information for parents and carers
- Supporting administrative tasks, such as creating templates, checklists or timetables
- Proofreading, improving the clarity of or restructuring text that you have written
- Generating ideas for displays, assemblies and enrichment activities.
- Supporting professional development, research and brainstorming

AI must NOT be used to:

- Enter confidential, sensitive or personally identifiable information about pupils, families or staff into an AI tool
- Enter any information about safeguarding concerns, SEND, medical needs, behaviour incidents, attendance, child protection matters or other sensitive pupil information into AI tools
- Make decisions about pupils, including decisions relating to safeguarding, behaviour, SEND, assessment, progress or support
- Replace professional judgement or the teacher–pupil relationship
- Produce or send communications containing inaccurate or unverified information
- Generate reports, assessments or professional judgements about pupils without the staff member checking and taking responsibility for the content
- Use AI-generated content without checking it for accuracy, bias, appropriateness and suitability for our pupils
- Upload copyrighted or confidential school materials to AI tools where we do not have permission to do so
- Use AI to create work that is presented as entirely our own when disclosure or acknowledgement is required
- Use AI in a way that breaches examination, coursework or assessment regulations

13. Educating parents and carers

The school will work in partnership with parents and carers to help pupils stay safe online at school and at home. Parents and carers will be provided with information about the school's approach to online safety and their role in protecting children.

Parents and carers will be made aware of risks including child sexual abuse and grooming; radicalisation and extremist content; sharing nudes or semi-nudes; AI-generated or altered sexual imagery and deepfakes; cyberbullying; pornography; harmful online communities and content; misinformation and disinformation; and online exploitation.

- Parents and carers will be informed about ways to reduce risks at home, including parental controls, age-appropriate settings, privacy settings, device security and having regular conversations about online activity.
- The school will signpost parents and carers to current DfE and other trusted guidance, including the government's online safety and mobile phone resources.
- Parental awareness will be raised through twilight training sessions, newsletters, online resources, individual advice and guidance conversations and targeted communication following significant incidents or emerging risks.

14. Filtering and monitoring online activity

The Management Committee has overall strategic responsibility for ensuring that appropriate filtering and monitoring systems are in place and that their effectiveness is reviewed at least once every academic year.

A named member of the senior leadership team, the DSL and relevant IT support will have clearly defined operational responsibilities for filtering and monitoring, with the responsible governor receiving appropriate assurance.

Compass School uses Smoothwall for filtering and monitoring. The school will ensure that filtering and monitoring are appropriate to pupils' age, risk profile, SEND/EAL needs, technology use and curriculum requirements, and that they do not unreasonably restrict teaching and learning.

The annual review will consider all school-managed internet-connected devices and relevant locations, including devices used off-site, BYOD arrangements where applicable, user-group profiles, safe-search arrangements, AI and generative-AI use, technical limitations and recent safeguarding incidents.

The school will keep a written record of the annual review and of routine checks, including when checks took place, who completed them, what was tested and any actions arising.

Monitoring arrangements will include regular review of monitoring reports, with weekly monitoring reports as a minimum and immediate escalation of high-risk safeguarding, malicious or technical incidents.

Requests to change filtering will be directed to the headteacher. The Network technician and DSL will complete a risk assessment before significant changes, and changes will be recorded.

All users will be informed about filtering and monitoring and why it is in place. Concerns identified through monitoring will be reported to the DSL and managed under the Child Protection and Safeguarding Policy.

Where illegal material is accessed, the school will follow the Child Protection and Safeguarding Policy and report to the appropriate agency, as required.

ICT technicians will undertake routine checks, with frequency determined by the school's risk assessment, and will work with the DSL/DDSL to investigate alerts and incidents.

15. Network security

Technical security features, such as anti-virus software, will be kept up-to-date and managed by Network technician. Firewalls will be switched on at all times. Network technician will review the firewalls on a weekly basis to ensure they are running correctly, and to carry out any required updates.

Staff and pupils will be advised not to download unapproved software or open unfamiliar email attachments and will be expected to report all malware and virus attacks to Network technician.

Users will be required to lock access to devices and systems when they are not in use.

16. Social networking

The use of social media by staff will be managed in line with the school’s Staff Code of conduct policy

17. The school website

The headteacher will be responsible for the overall content of the school website – they will ensure the content is appropriate, accurate, up-to-date and meets government requirements.

This policy will be reviewed during the 2026–2027 academic year in response to changes in statutory guidance, legislation, technology and the school's safeguarding risk profile.

18. Use of devices

Staff members and pupils will be issued with school-owned devices to assist with their work, where necessary. Requirements around the use of school-owned devices can be found in the Staff Code of conduct policy

The use of personal devices on the school premises and for the purposes of schoolwork will be managed in line with the Staff Code of conduct policy