

Carlton Digby School



Online Safety Policy

Including:
Social Media Policy
Cybersecurity Policy

2025 – 2026

Policy reviewed by	<i>Naomi Boulter</i>
Date of policy review	10.10.2025
Date approved by Governors	02.12.2025
Date of next review	October 2026

Contents

Key people	1
Section 1: Online Safety Policy	2
1. Introduction	2
2. The main online safety risks in 2025 – 2026?	2
3. Communication of this policy	3
4. Overview	3
4.1 Aims	3
4.2 Further Help and Support	3
4.3 Scope	4
5. Roles and responsibilities	4
5.1 All staff	4
5.2 Head Teacher	4
5.3 Designated Safeguarding Leads / Online Safety Lead	5
5.4 Governing Body / Safeguarding Link Governor	5
5.5 PSHE / RSHE Lead	6
5.6 Computing Lead	6
5.7 Subject Leaders	6
5.8 IT Technician and ATOM IT	6
5.9 Data Protection Officer (DPO)	7
5.10 Volunteers and contractors (including tutors)	7
5.11 Pupils	7
5.12 Parents/carers	7
5.13 External groups	8
6. Education and curriculum	8
7. Handling safeguarding concerns and incidents	8
7.1 Actions where there are concerns about a child	9
7.2 Sexting – sharing nudes and semi-nudes	10
7.3 Upskirting	11
7.4 Bullying	11
7.5 Child-on-child sexual violence and sexual harassment	12
7.6 Misuse of school technology (devices, systems, networks or platforms)	12
7.7 Social media incidents	12
7.8 CCTV	12
7.9 Extremism	12
8. Data protection and cybersecurity	12
9. Appropriate filtering and monitoring	12
9.1 Filtering and Monitoring Systems	13
9.2 Mobile and Device Management	13
10. Messaging/commenting systems	13
10.1 Authorised systems	13
10.2 Behaviour / usage principles	14
11. Use of generative Artificial Intelligence	14

12.	Online storage or learning platforms	15
13.	School website	15
14.	Digital images and video	15
15.	Device usage	16
15.1	Personal devices including wearable technology and bring your own device	16
15.2	Use of school devices	16
15.3	Trips / events away from school	17
15.4	Searching and confiscation	17
Section 2: Social Media Policy		18
1.	Our social media presence	18
2.	Staff, pupils' and parents' social media presence	18
3.	Social media incidents	19
4.	Extremism	19
Section 3: Cybersecurity Policy		20
1.	Introduction	20
2.	Scope of Policy	20
3.	Risk Management	20
4.	Physical Security	20
5.	Asset Management	20
6.	User Accounts	20
7.	Devices	20
8.	Data Security	21
9.	Sharing Files	21
10.	Training	21
11.	System Security	22
12.	Major Incident Response Plan	22
13.	Maintaining Security	22
Appendix: Acceptable Use Policy Agreement		23
1.	Pupils	23
2.	Staff and Governors	25

Key people

Designated Safeguarding Lead (DSL), with lead responsibility for filtering and monitoring	Naomi Boulter – Head Teacher
Deputy Designated Safeguarding Leads	Brett Meats – Deputy Head Teacher Tricia Marron – Assistant Head Teacher Rachel Saunders – Assistant Head Teacher
Link governor for safeguarding	Rachel Edworthy
Curriculum leads with relevance to online safeguarding and their role	PSHE / RSHE lead – Helen Fitzmaurice Computing lead – Danielle Rigg
IT Technician / other technical support	ATOM IT – technical support

Section 1: Online Safety Policy

1. Introduction

Online safety is a core element of safeguarding and requires a whole-school, cross-curricular approach involving collaboration across all key leadership areas.

This policy is written in line with Keeping Children Safe in Education (KCSIE) 2025, Teaching Online Safety in Schools, statutory RSHE guidance, and other relevant legislation. It applies across the curriculum—not only to RSHE, Citizenship, and Computing—and should be read alongside the Child Protection and Safeguarding Policy.

All online safety concerns must be managed in accordance with the school’s safeguarding and child protection procedures.

This policy is reviewed annually and updated as needed in response to school or local developments. Staff, governors, pupils, and parents are involved in review to ensure it is practical, understood, and applied consistently. Pupil-friendly versions and stakeholder Acceptable Use Policies should be reviewed at the same time, and any updates shared promptly with all parties.

KCSIE 2025 states that the Designated Safeguarding Lead (DSL) holds overall responsibility for safeguarding and child protection, including online safety. While specific tasks may be delegated, the DSL retains overall accountability.

Subject coordinators, such as those for RSHE, must ensure their curriculum supports and aligns with the school’s whole-school safeguarding approach.

2. The main online safety risks in 2025 – 2026?

KCSIE 2025 states that schools must address misinformation and disinformation online as part of safeguarding under the four risk categories:

1. **Content** — illegal, inappropriate or harmful content (now explicitly including misinformation, disinformation, conspiracy theories)
2. **Contact** — harmful interaction with others
3. **Conduct** — pupils’ own online behaviour
4. **Commerce** — online financial scams, advertising, etc.

In the past year, we have seen:

- Inappropriate online searches
- Increased mobile phone use for gaming and social media

2.1 National and local trends reflect similar concerns, linked to the 4 Cs (content, contact, conduct, commerce).

Generative AI is now widely accessible and presents risks including misinformation, plagiarism, and inappropriate or sexualised content. Many tools lack safety settings and are unsuitable for under-13s. Schools must teach pupils and parents safe, responsible use.

Social media use continues to rise. Ofcom’s 2024 report shows most under-18s use YouTube, TikTok, Snapchat or WhatsApp, often below age limits. Many children spend over three hours online

daily, and half of under-13s admit to creating fake-age profiles, increasing exposure to harmful content.

Device access is widespread: most pupils have personal smartphones by Year 7, many without safety controls. The Internet Watch Foundation reports a sharp increase in self-generated child sexual abuse material among 11–13-year-olds, including cases of sextortion affecting boys and girls.

Misinformation online is a growing concern. The 2024 Southport incident highlighted how false content shared on social media can rapidly incite hate and violence. Schools must help pupils critically assess information sources.

There have also been safeguarding issues involving parents filming staff or pupils and posting videos online, putting children and the school community at risk.

Cyber security remains a significant threat, with most schools reporting attempted attacks. Online safety now includes maintaining robust digital security as part of safeguarding practice.

3. Communication of this policy

It will be communicated in the following ways:

- Posted on the school website
- School induction pack for all new staff (including temporary, supply and non-classroom-based staff and those starting mid-year)
- Safeguarding updates and training for all staff
- Acceptable Use Policies (AUPs) for staff, volunteers, contractors, governors, pupils and parents/carers, written in accessible language

4. Overview

4.1 Aims

This policy promotes a whole-school approach to online safety by:

- Defining clear expectations for all members of the Carlton Digby School community in their online behaviour, use of digital technology, and social media activity, both in and outside school.
- Supporting safeguarding and leadership teams to maintain awareness of online risks through effective collaboration with technical staff (e.g. filtering and monitoring) and curriculum leads (e.g. RSHE).
- Ensuring consistent standards of behaviour online and offline.
- Promoting the safe, responsible and positive use of technology to enhance learning and prepare pupils for life in a digital world.
- Helping staff understand their responsibilities to:
 - Protect and support pupils' wellbeing online;
 - Protect themselves from misuse or allegations;
 - Uphold the school's ethos and reputation.
- Setting out clear procedures for managing online incidents, with links to related policies such as Behaviour and Anti-Bullying.

4.2 Further Help and Support

All concerns must be reported through internal school procedures, in line with the Child Protection and Safeguarding Policy. The DSL manages referrals to the Local Authority MASH, and the Head Teacher handles referrals to the LADO. External advisors from the local authority, trust, or partner agencies may provide additional guidance.

Further support is available via reporting.lgfl.net, which lists external helplines including the Professionals' Online Safety Helpline, NSPCC Report Abuse Helpline, and services for hate crime, terrorism, fraud, and anonymous child support.

4.3 Scope

This policy applies to all members of the Carlton Digby School community, including staff, governors, volunteers, contractors, pupils, parents/carers, visitors, and community users, who access or use the school's digital technology, networks, or systems, whether on-site or remotely, and at any time as part of their school role.

5. Roles and responsibilities

The school community shares a collective duty to act respectfully online and offline, use technology responsibly, and report any concerns or inappropriate behaviour to protect pupils, staff, families, and the school's reputation.

All members should read the sections relevant to their role. The **All Staff** section applies to everyone, alongside additional guidance for specific roles (e.g. DSL, governors, pupils) in the annex. Staff are expected to remain vigilant and report any emerging issues or risks.

5.1 All staff

All staff must follow the Staff Acceptable Use Policy, the Safeguarding Policy, the Code of Conduct, and relevant sections of KCSIE, as part of a whole-school safeguarding approach.

Staff must report all concerns, however minor, to the Designated Safeguarding Lead (DSL) and remain informed about current online safety issues and guidance. They should model safe, responsible, and professional use of technology and avoid using language that blames or frightens pupils.

Staff must understand the DfE Filtering and Monitoring Standards, report issues such as overblocking or system gaps, and actively supervise pupils' online activity during lessons.

5.2 Head Teacher

Key responsibilities:

- Embed online safety within the whole-school safeguarding culture.
- Oversee and support the DSL team, ensuring collaboration with technical staff to complete an annual online safety audit in line with KCSIE.
- Complete safeguarding training (including online safety) and ensure all staff and governors receive regular updates.
- Provide strategic oversight, ensuring policies and practice are effective and up to date.
- Ensure safe and compliant use of ICT systems, including secure filtering, monitoring, and remote access.
- Review and understand filtering and monitoring decisions with the DSL and technical staff, as required by DfE standards.
- Liaise regularly with the DSL on online safety matters and receive termly updates.
- Support safeguarding and technical staff in reviewing protections for home and remote learning.
- Oversee data management and information security, working with the DPO, DSL, and governors to balance data protection with effective safeguarding.
- Ensure all staff understand procedures for serious online incidents.

- Oversee risk assessments to address online risks, including radicalisation.
- Ensure the school website meets all statutory requirements.

5.3 Designated Safeguarding Leads / Online Safety Lead

The Designated Safeguarding Lead (DSL) holds overall responsibility for safeguarding and child protection, including online safety. Tasks may be delegated, but accountability cannot.

- Lead on a whole-school approach to online safety in line with KCSIE 2025.
- Ensure compliance with DfE Filtering and Monitoring Standards, including annual testing and review, with findings reported to governors.
- Work with technical staff to review filtering and monitoring systems, document outcomes, and agree appropriate access levels (e.g. YouTube mode, search engine settings).
- Ensure online safety is embedded across the curriculum (e.g. RSHE) and that messages to pupils are consistent.
- Provide and update safeguarding and online safety training for all staff, supply staff, and governors, including induction and regular refreshers.
- Ensure staff read KCSIE Part 1 and, where relevant, Annex B, and understand their roles in identifying and reporting online risks.
- Oversee day-to-day safeguarding operations, ensuring appropriate, non-judgemental language is used when managing concerns.
- Review remote learning procedures to ensure online safety and behaviour expectations remain consistent.
- Work with the Headteacher, DPO, and governors to maintain secure data management and lawful information sharing that prioritises child protection.
- Stay informed on emerging online risks, trends, and legal developments, including Prevent requirements.
- Regularly review and update this policy, Acceptable Use Policies, and related documents to ensure alignment with wider safeguarding policies.
- Promote online safety awareness across the whole school community, including parents and carers.
- Meet regularly with the SLT and safeguarding governor to review incidents, filtering logs, and practice effectiveness.
- Ensure staff and pupils know how to report online incidents and that all are recorded as safeguarding concerns.
- Provide clear systems for reporting issues both in and outside school.
- Enforce a zero-tolerance approach to child-on-child abuse, including bullying and harmful online behaviour.

5.4 Governing Body / Safeguarding Link Governor

Key responsibilities:

- Approve this policy and review its effectiveness, using the UKCIS Online Safety in Schools and Colleges: Questions from the Governing Board as a reference.
- Undertake safeguarding and child protection training, including online safety, at induction and through regular updates, and ensure all staff do the same.
- Appoint a named governor for filtering and monitoring to work closely with the DSL in meeting DfE standards.
- Engage parents and the wider community in online safety initiatives.
- Hold regular strategic reviews with the DSL/online safety lead and include online safety within routine safeguarding discussions.
- Work with the Headteacher, DSL, and DPO to ensure secure data management that prioritises child protection and lawful information sharing.

- Confirm all staff have read KCSIE Part 1, and that SLT and staff working directly with children have read Annex B.
- Ensure online safety education is embedded across the curriculum and that there is a clear, consistent policy on the use of mobile technology.

5.5 PSHE / RSHE Lead

Key responsibilities:

- In addition to the responsibilities listed under All Staff:
- Embed teaching on consent, mental wellbeing, healthy relationships, and online safety within PSHE, RSHE, and Health Education. This includes addressing risks linked to AI-generated content, financial extortion, and sharing intimate images.
- Teach pupils what positive and respectful online relationships look like, the impact of online behaviour, and how to act safely and appropriately.
- Deliver the Teaching Online Safety in Schools framework in an age-appropriate way, helping pupils navigate digital spaces confidently and safely.
- Assess understanding through classwork, reflection, or discussion to identify pupils needing additional support.
- Work closely with the DSL, Computing Lead, and other staff to ensure consistent messaging and a joined-up whole-school approach.
- Ensure the RSHE Policy is published on the school website.

5.6 Computing Lead

Key responsibilities:

- In addition to the responsibilities in the All Staff section:
- Lead and oversee delivery of the online safety strand of the Computing curriculum in line with the National Curriculum.
- Work with the RSHE Lead to ensure a consistent, whole-school approach without duplication.
- Liaise with the DSL and wider staff to maintain clear, consistent messaging around online safety.
- Collaborate with technical staff to ensure ICT use aligns with school Acceptable Use Agreements and safeguarding principles.

5.7 Subject Leaders

Key responsibilities:

- In addition to the responsibilities in the All Staff section:
- Embed online safety themes within your subject, particularly through RSHE, and model positive digital behaviour.
- Apply relevant guidance from Education for a Connected World and Teaching Online Safety in Schools.
- Work with the DSL and colleagues to maintain consistent messaging across subjects.
- Include an online safety focus in subject action plans.

5.8 IT Technician and ATOM IT

Key responsibilities:

- In addition to the responsibilities in the All Staff section:
- Work with the DSL and SLT to inform strategic decisions on the safeguarding aspects of technology.

- Support the DSL in managing, reviewing, and documenting filtering and monitoring systems, ensuring compliance with DfE standards and avoiding overblocking.
- Assist with the annual online safety audit, including reviews of filtering, monitoring, and remote learning protections.
- Stay up to date with the Online Safety Policy and ensure school systems reflect safeguarding requirements.
- Collaborate with the DSL, DPO, and RSHE Lead to ensure consistent practice across safeguarding, curriculum, and technology use.
- Explain the implications of system changes (e.g. access levels, web filtering, file sharing permissions) to relevant staff.
- Test new devices and systems for compliance before deployment.
- Maintain accurate documentation of online security and technical procedures.
- Report any online safety concerns in line with school policy.
- Manage networks, passwords, and data securely, ensuring protection, encryption, backup, and recovery systems are in place.
- Keep the Data Protection and Cybersecurity Policies current, practical, and accessible.
- Monitor the use of school technology and promptly report any misuse or attempted breaches.

5.9 Data Protection Officer (DPO)

Key responsibilities:

- Provide data protection expertise, training, and oversight to ensure the Data Protection and Cybersecurity Policies align with legislation and this policy.
- Support safe information sharing, recognising that GDPR and the Data Protection Act 2018 do not prevent sharing data to safeguard children. Consent is not required when sharing for child protection purposes.
- Apply appropriate retention periods for safeguarding records (typically until the pupil is at least 25).
- Restrict, monitor, and audit access to safeguarding data to maintain security and confidentiality.

5.10 Volunteers and contractors (including tutors)

Key responsibilities:

- Read, understand, sign, and follow the Acceptable Use Policy (AUP).
- Report all concerns, however minor, to the Designated Safeguarding Lead (DSL).
- Stay informed about current online safety guidance and issues.
- Model safe, responsible, and professional use of technology, including during remote teaching or online communication.
- Never arrange meetings, tutoring sessions, or private communications with pupils without prior school approval, in line with the AUP.

5.11 Pupils

Key responsibilities:

- Read, understand, sign and adhere to the pupil acceptable use policy if appropriate.

5.12 Parents/carers

Key responsibilities:

- Read and adhere to the school's parental acceptable use policy (AUP), read the pupil AUP and encourage their children to follow it.

5.13 External groups

Key responsibilities:

- All external visitors or organisations must sign an Acceptable Use Policy (AUP) before using school technology or accessing the internet.
- Support the school's approach to online safety and data protection.
- Model respectful, responsible, and positive online behaviour, including on social media—never sharing others' images or information without consent or posting negative or harmful comments about members of the school community.

6. Education and curriculum

Carlton Digby School recognises that, while the online world carries risks, it also offers significant opportunities for learning, communication, and independence. Technology use in school is guided by pedagogy and inclusion.

The school delivers a sequenced online safety curriculum that develops pupils' digital competence and understanding of online risks, matched to their age and stage of development. Teaching focuses on the knowledge, skills, and behaviours pupils need to navigate the online world safely, confidently, and respectfully.

Online safety is embedded across the curriculum in line with Teaching Online Safety in Schools, with clear links to:

- RSHE
- PSHE
- Computing
- Citizenship

All staff share responsibility for reinforcing online safety in every aspect of school life and taking advantage of spontaneous learning opportunities. When using technology in lessons or for homework, staff should ensure age-appropriate use, model safe behaviour, and support pupils in:

- Using search tools and sources critically (e.g. recognising misinformation)
- Reporting concerns or seeking help
- Understanding age-appropriate content, copyright, and data protection

The school follows the Education for a Connected World (UKCIS, 2020) framework to develop pupils' digital resilience and reviews curriculum plans annually, including for SEND learners, as part of the whole-school online safety audit.

Parents and carers are kept informed about online safety learning and activities through the school website, ClassDojo, and newsletters.

7. Handling safeguarding concerns and incidents

KCSIE 2025 confirms that low-level concerns related to digital or online conduct must be recorded and reviewed in line with the Staff Behaviour and Low-Level Concerns Policy.

Online safety is a core part of safeguarding. All concerns, however small, must be reported to the Designated Safeguarding Lead (DSL). Every piece of information helps build a full safeguarding picture, and support staff often have valuable insights from informal settings such as playgrounds and corridors.

Online safety procedures are detailed in the following key policies:

- Safeguarding and Child Protection Policy
- Child-on-Child Abuse Policy
- Anti-Bullying Policy
- Behaviour Policy
- Acceptable Use Policies (AUPs)
- Prevent Risk Assessment
- Data Protection Policy and related documentation
- Cyber Security Policy

The school takes all reasonable steps to safeguard pupils online but recognises incidents may occur inside and outside school. All members of the community are encouraged to report issues promptly so they can be addressed swiftly and sensitively.

Any suspected online risk or incident must be reported to the DSL on the same day (or by the end of the lesson if urgent) and recorded on MyConcern, including alerts generated by filtering or monitoring systems.

Concerns about staff misuse are reported directly to the Head Teacher. If the concern involves the Head Teacher, it must be referred to the Chair of Governors. Staff can also contact the NSPCC Whistleblowing Helpline.

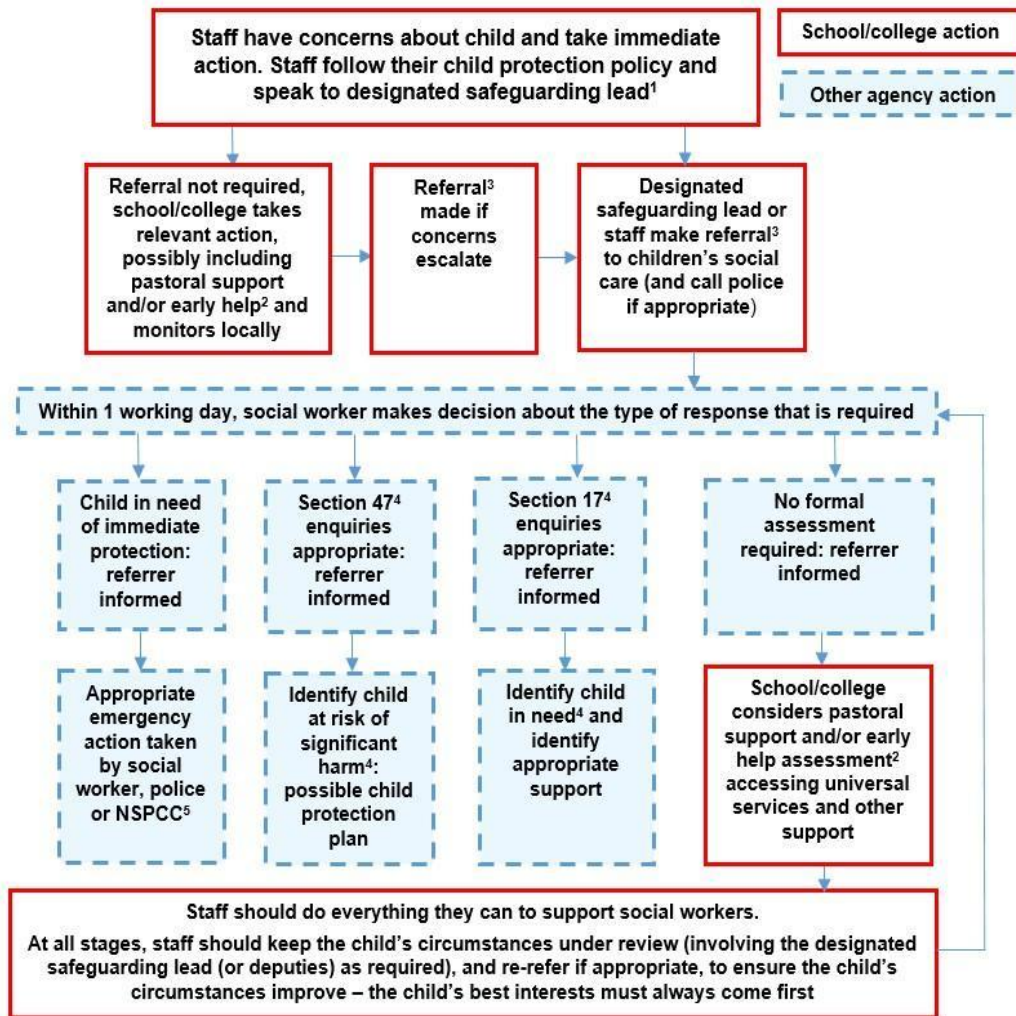
The school will seek support from relevant external agencies where necessary, such as the Local Authority, UK Safer Internet Centre (POSH), CEOP, Prevent, Police, IWF, or the Harmful Sexual Behaviour Support Service.

Parents and carers will be informed of any online safety incidents involving their child, and the Police will be contacted where behaviour is illegal or presents serious concern.

The school will regularly review reporting systems to ensure they remain effective, including during any future closures or periods of remote learning.

7.1 Actions where there are concerns about a child

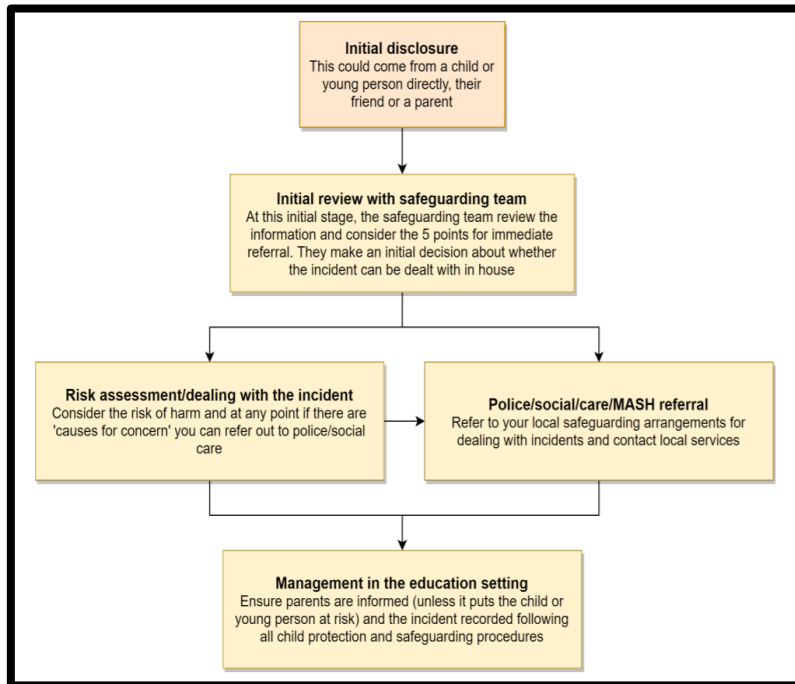
The following flow chart is taken from Keeping Children Safe in Education 2025. Online safety concerns are no different to any other safeguarding concern.



7.2 Sexting – sharing nudes and semi-nudes

All schools must follow the UKCIS guidance Sharing nudes and semi-nudes: advice for education settings. A one-page summary, How to Respond to an Incident, should be read by all staff, as incidents are often first discovered by someone other than the DSL. Staff must not view, share, copy, or delete any image, nor ask others to do so. They should report the concern immediately to the DSL.

While sharing nudes involving children is illegal, pupils should feel able to seek help without fear of blame or criminalisation. The UKCIS guidance promotes a supportive, proportionate response focused on safeguarding, not punishment. The DSL will use the full UKCIS guidance to determine next steps, including whether to involve external agencies, contact parents, or provide further pupil support.



The following LGfL document (available at nudes.lgfl.net) may also be helpful for DSLs in making their decision about whether to refer a concern about sharing of nudes:

SAFEGUARDING QUESTION TIME

Q: WHEN SHOULD WE REFER NUDE SHARING?
A: IMMEDIATELY *IF* THE IMAGE/VIDEO:

- involves an adult
- is potentially coerced, blackmailed or groomed or concerns about capacity to consent
- might depict sexual acts unusual for their developmental stage or violent
- involves sexual acts / under 13s
- or the young person is at immediate risk of harm[...], suicidal or self-harming

Text simplified, taken from page 20 of 'Sharing Nudes and Semi-Nudes', UKCIS – search.gov.uk

"We recommend DSLs read the entire UKCIS document; there is much more to know than this, and many helpful resources including training, scenarios and further guidance. Note also the one-pager for all staff!"

LGfL
SafeguardED

7.3 Upskirting

Upskirting (taking photos under someone’s clothing without consent) is a criminal offence and a form of sexual harassment under KCSIE 2025. Pupils are encouraged to speak to staff if they have concerns or have made a mistake in this area.

7.4 Bullying

Online bullying (cyberbullying), including incidents outside school, will be addressed under the Anti-Bullying Policy and treated as any other form of bullying. Staff should be aware that incidents may involve filming, live streaming, or the use of fake profiles.

7.5 Child-on-child sexual violence and sexual harassment

All incidents of sexual harassment or violence, online or offline, must be reported to the DSL and handled according to KCSIE 2025.

Staff should maintain a zero-tolerance approach, recognising that all behaviours on the continuum, from inappropriate comments to physical assault, must be taken seriously and never dismissed as “banter.”

7.6 Misuse of school technology (devices, systems, networks or platforms)

Rules for the safe use of school technology, networks, and devices are detailed in the Acceptable Use Policies (AUPs) and this policy.

- Pupil breaches are dealt with under the Behaviour Policy.
- Staff breaches are dealt with under the Code of Conduct.
- Pupils are reminded of these rules regularly, including during home learning.

The school reserves the right to withdraw access to technology or personal devices where rules are breached.

7.7 Social media incidents

Social media incidents involving pupils are treated as safeguarding concerns and handled under the Safeguarding, Online Safety, and Acceptable Use Policies. Posts that are inappropriate, abusive, or defamatory towards staff, pupils, or the school will be requested for immediate removal. If posted by a third party, the school may report the content to the platform and seek advice from the Professionals’ Online Safety Helpline (POSH).

7.8 CCTV

CCTV is used around the school perimeter to maintain safety. Footage is securely stored, accessed only by authorised staff or the police, and managed under the GDPR Policy. No consent is required for this use.

7.9 Extremism

Under the Prevent Duty, the school will not support or promote extremist views or materials. Staff and parents are reminded that extremist and hate content can circulate on social media, and vigilance is required both in and outside school.

8. Data protection and cybersecurity

All pupils, staff, governors, volunteers, contractors, and parents must follow the school’s Data Protection and Cybersecurity Policies. These are integral to effective safeguarding, as highlighted in KCSIE 2025 and the DfE Cybersecurity Standards.

Data protection laws do not prevent sharing information to keep children safe. As stated in Data Protection in Schools (2023) and KCSIE 2025, consent is not usually required when sharing personal information for safeguarding purposes. Staff must never allow concerns about data sharing to delay or prevent action that protects a child’s welfare.

9. Appropriate filtering and monitoring

The Designated Safeguarding Lead (DSL) has overall responsibility for filtering and monitoring and works with ATOM IT to meet DfE Filtering and Monitoring Standards, which require schools to:

- Assign clear roles and responsibilities;
- Review provision at least annually;

- Block harmful or inappropriate content without restricting learning;
- Implement effective, risk-based monitoring strategies.

Carlton Digby School provides appropriate filtering and monitoring at all times, as outlined in KCSIE 2025. All staff are informed about these systems during induction, annual safeguarding training, and via Acceptable Use Policies (AUPs). They are expected to report concerns such as overblocking, bypass attempts, or system gaps to the DSL at any time. The DSL receives and reviews regular filtering reports and takes appropriate action. Technical and safeguarding staff conduct half-termly checks and an annual online safety audit to ensure systems are effective and support teaching and learning.

9.1 Filtering and Monitoring Systems

- Provided by ATOM IT and Securly (on-site and for school devices used at home).
- Changes managed by the Head Teacher and ATOM IT.
- Overall responsibility held by the DSL, supported by SLT.
- Technical configuration and maintenance by ATOM IT.
- Half-termly checks ensure functionality and coverage.
- Annual review forms part of the school's online safety audit.

Monitoring Methods (as outlined in DfE standards) may include:

- Staff supervision and physical screen monitoring;
- Device management software for live oversight;
- Network log reviews and alerts;
- Automated monitoring tools (e.g. Securly) for off-site protection.

Safe Search and YouTube restrictions are enforced across all devices. Out-of-hours filtering applies to staff devices through Securly, with alerts sent directly to DSLs.

9.2 Mobile and Device Management

- All school devices are managed through Mobile Device Management (MDM) software with role-based access controls.
- Internet filtering applies to all connections; bypassing restrictions is prohibited.
- Broadband capacity is maintained to support educational use.
- Staff must electronically sign for devices, confirming compliance with school policies.
- Devices are subject to real-time and periodic monitoring (both on and off site).
- Devices may be recalled periodically for inspection by designated staff.
- Equipment must be returned when staff leave or take extended absence (e.g. illness or parental leave).

Returned devices are processed and reallocated by the Office or Computing TA.

10. Messaging/commenting systems

10.1 Authorised systems

Pupils may communicate through Purple Mash or school email where appropriate.

Staff use the Office 365 email system for all school communication. Personal email accounts or private messaging platforms must never be used for contacting pupils, parents, or colleagues about school matters or pupil data. Staff may email external organisations only for legitimate work purposes.

ClassDojo is used for communication with parents and is centrally managed and monitored by the Senior Leadership Team (SLT). Exclusive staff accounts (e.g. Head Teacher) are only created when necessary and approved by SLT.

All communication systems are centrally administered and monitored by the school or authorised IT partners to ensure transparency, safeguard pupils and staff, and comply with UK data protection legislation.

Use of any new platform involving communication, pupil logins, or school data must be approved in advance by SLT and, where relevant, authorised by the Head Teacher (especially for systems linked to the school's MIS).

Unauthorised use of alternative systems may be treated as a safeguarding or disciplinary matter and must be reported to the DSL (if by a pupil) or the Head Teacher (if by staff).

If a private account is used accidentally for school communication or data storage, the DSL, Head Teacher, or DPO must be notified immediately.

10.2 Behaviour / usage principles

Further guidance on these points can be found in the Social Media section, Acceptable Use Agreements, Behaviour Policy, and Staff Code of Conduct.

All users are expected to behave appropriately at all times. School communication systems must never be used to send messages or materials that are offensive, abusive, illegal, or otherwise inappropriate, or that could bring the school into disrepute.

All communication must comply with data protection principles and the Data Protection Policy, using only approved school systems.

Personal use of school email is not permitted. All emails are monitored, and inappropriate content (e.g. offensive language, images, or links to adult sites) may be blocked and dealt with under the relevant policy or procedure.

11. Use of generative Artificial Intelligence

In line with KCSIE 2025 and DfE guidance, Carlton Digby School recognises both the opportunities and risks associated with generative AI tools (e.g. ChatGPT).

- AI tools must never process or store identifiable pupil data.
- AI use must consider data protection, age-appropriate access, and the risk of misinformation or bias.
- The school will engage pupils, staff, and parents in discussions about AI use, focusing on its educational benefits and ethical implications.
- We recognise that pupils may encounter AI tools at home, and this may include both positive and harmful experiences (e.g. exposure to misinformation, deepfakes, bullying, or inappropriate content).
- The use of AI to cheat or plagiarise, including in exams or assessed work, is strictly prohibited and will be dealt with under the Behaviour Policy.
- Staff may use AI to support teaching and learning, provided it is used responsibly, aligns with safeguarding principles, and complies with data protection legislation.

12. Online storage or learning platforms

All principles above apply to any online system used for school business, whether for file storage, data management, collaboration, or teaching. When using such platforms, staff, governors, and volunteers must follow the school's Cybersecurity and Data Protection Policies, ensuring all activity complies with safeguarding and data security requirements.

13. School website

The school website serves as a key communication and information platform for the school community and holds significant reputational value. The Head Teacher and Governors delegate responsibility for website updates and DfE compliance to the Deputy Head Teacher and Office Staff. The site is hosted by e4education.

All staff submitting content must follow copyright law. Only use materials with permission or from open-access/public-domain sources, and always credit original creators. Finding content online (e.g. via Google or YouTube) does not guarantee it is copyright-free. When unsure, staff should seek guidance from a member of the Senior Leadership Team (SLT).

14. Digital images and video

When pupils join the school, parents and carers are asked to give consent for the use of their child's image or video. Consent specifies purpose (beyond internal assessment, which does not require explicit consent) and duration. Parents may approve use for:

- School displays
- ClassDojo updates
- Newsletters
- Printed marketing materials
- The school website or prospectus
- Social media
- Specific high-profile publications or displays

Staff must check the consent database before using any photo or video. Pupils featured in public materials are identified by first name only, and file names must not include full names.

Staff must follow the Acceptable Use Policy and Data Protection Policy regarding the capture and storage of images. Personal phones must never be used to take photos or videos of pupils; school-issued iPads or iPhones must be used instead, including during off-site activities.

All photos are stored securely on OneDrive in accordance with the school's data retention schedule. Any concerns about imagery or potential misuse must be reported immediately to the DSL.

Staff and parents are reminded annually not to share images without permission due to child protection, data protection, cultural, or privacy reasons.

Pupils are taught about:

- The risks of oversharing and managing their digital footprint
- How images can be edited or misused
- Respecting others' privacy and seeking consent before sharing images
- Using privacy settings and secure data practices
- How to respond if they or a peer experience online bullying or image-based abuse

15. Device usage

Acceptable Use Policies (AUPs) outline expectations for all users of school devices. Devices used at home must be treated as if they were in full view of colleagues or pupils. This section should be read alongside related policies, including those on copyright, data protection, social media, misuse of technology, and digital images.

Liability for Damage

- Damage occurring in school is covered under the school's insurance policy.
- Users must take reasonable care to prevent damage, including using protective cases and screens.
- Devices should be transported safely and kept away from food or drinks.
- When devices are taken off-site, staff must ensure their personal home insurance covers loss or damage. If not, they may be liable for repair or replacement costs.

15.1 Personal devices including wearable technology and bring your own device

Pupils may bring mobile phones to school but must hand them to the office on arrival and collect them at the end of the day. Phones must not be kept on their person or used in classrooms. Where a pupil requires a phone temporarily for regulation purposes (e.g. on transport), it must be handed in at the earliest opportunity. Important messages or calls can be made or received via the school office, which will contact pupils in emergencies.

Staff must keep personal phones on silent and only use them in designated staff areas during school hours. Child or staff data must never be stored or accessed on personal devices. If a staff member is expecting an urgent personal call, they must seek permission from the Senior Leadership Team (SLT) and take the call away from pupil areas.

Volunteers, Contractors, and Governors personal phones must remain switched off and out of sight. They must not be used in the presence of pupils or for taking photos/videos. Where photography is required for work purposes (e.g. site maintenance), permission must be obtained from the Head Teacher and carried out in the presence of staff.

Parents and Carers should keep phones on silent while on site and seek permission before taking any photos (e.g. of displays), ensuring no other pupils are included. During events, parents must follow the guidance in the Digital Images and Video section. Parents should not contact pupils directly during the school day; urgent messages must go through the school office.

15.2 Use of school devices

Staff and pupils must follow the Acceptable Use Policies (AUPs) and Staff Code of Conduct when using school devices, on-site or at home. Devices must never be used in ways that breach these policies.

Wi-Fi access is available to visitors for school-related purposes only and is subject to the same filtering, monitoring, and acceptable use standards as school devices.

School-issued devices are limited to approved apps and software installed by the school and may be used for learning and reasonable, appropriate personal use.

All device and network activity is monitored and logged in line with safeguarding and data protection requirements.

15.3 Trips / events away from school

For all trips and off-site activities, staff will be issued a school duty phone for authorised and emergency communication with pupils or parents. Any unavoidable use of a personal phone (e.g. technical failure of the school device) must be reported immediately to the Head Teacher. In such cases, staff must withhold their personal number to protect privacy.

15.4 Searching and confiscation

In line with the DfE guidance Searching, Screening and Confiscation: Advice for Schools, the Head Teacher and authorised staff have the legal power to search pupils or their property, including mobile phones and other devices, where there is reasonable suspicion of illegal or inappropriate content (e.g. sexual images, pornography, violence, or bullying).

Section 2: Social Media Policy

1. Our social media presence

Carlton Digby School recognises that managing its online reputation is essential to safeguarding its community and maintaining public confidence. The school actively monitors its digital footprint to ensure that information shared online is accurate and that any concerns are addressed swiftly and appropriately. The school's Facebook page is managed by members of the Senior Leadership Team (SLT) and the Family Support Worker. All content reflects the school's values and safeguarding commitments.

2. Staff, pupils' and parents' social media presence

Social media, including all platforms, apps, and games allowing interaction, is part of modern life. However, all members of the school community are expected to engage respectfully and responsibly, in line with the Acceptable Use Policy (AUP), Behaviour Policy, and Staff Code of Conduct. Posts must never include content that is bullying, abusive, rude, illegal, discriminatory, or that could bring the school or the teaching profession into disrepute. This applies to both public and private online spaces.

Parents are asked to raise concerns directly with the school rather than through social media. The Complaints Policy outlines how issues can be resolved constructively. Public sharing of grievances online can damage staff morale and the school's reputation.

Most social media platforms have a minimum age of 13; parents are encouraged to respect age restrictions and discuss online behaviour and safety regularly with their children. Helpful tools include:

- Digital Family Agreement
- Top Tips for Parents Poster
- ParentSafe (parentsafe.lgfl.net)
- Children's Commissioner's Digital 5 a Day

The school's official communication channels with parents are email and Class Dojo. Social media (including WhatsApp) must not be used for direct school communication.

Boundaries Between Staff and Pupils

- Pupils must not attempt to connect with staff, governors, volunteers, or contractors via social media.
- Staff and associated adults must not send or accept friend/follow requests from pupils.
- Exceptions (e.g. pre-existing family relationships) must be declared and approved by the Head Teacher.

Staff are reminded that maintaining strict privacy settings and avoiding discussions about the school online help protect both professional integrity and safeguarding standards. The Teacher Regulation Agency has issued prohibition orders for misuse of social media—highlighting the seriousness of such breaches.

All community members must comply with the Digital Images and Video Policy and seek consent before posting photos, videos, or personal information about others. Parents must not covertly record staff or pupils, or share images of other children online, as this may pose safeguarding or legal risks.

3. Social media incidents

Social media incidents involving pupils are treated as safeguarding concerns and managed under the Safeguarding, Online Safety, and Acceptable Use Policies. Pupil breaches are addressed under the Behaviour Policy. Staff breaches are addressed under the Code of Conduct.

If an inappropriate, offensive, or harmful post is made by a member of the school community, the school will request its immediate removal. Posts made by third parties may be reported to the platform and, if necessary, referred to the Professionals' Online Safety Helpline (POSH) or the Police if illegal or harmful.

4. Extremism

Under the Prevent Duty, the school has a legal obligation to protect pupils from radicalisation and extremist material. Staff must not promote or engage with extremist organisations or content and must report any concerns to the DSL. Parents are asked to support this approach, particularly given the prevalence of extremist and hate content on social media.

Section 3: Cybersecurity Policy

1. Introduction

A cybersecurity incident can significantly disrupt school operations, from reputational damage and system recovery costs to the loss of pupil work, access to learning platforms, or safeguarding data, potentially resulting in data protection breaches or inspection failures. This Cybersecurity Policy sets out Carlton Digby School's procedures and security measures to protect systems, services, and data, and to ensure an effective response in the event of a cyberattack.

2. Scope of Policy

This policy applies to all Carlton Digby School staff, contractors, volunteers, and anyone granted temporary or permanent access to the school's systems or hardware. It also covers the physical and technical infrastructure used to deliver the school's IT services.

3. Risk Management

Carlton Digby School will include cybersecurity risks on its organisational risk register, regularly reporting on the progress and management of these risks to Governors at least once per year.

4. Physical Security

Carlton Digby School will ensure there is appropriate physical security and environmental controls protecting access to its IT Systems, including but not limited to air conditioning, lockable cabinets, and secure server/communications rooms.

5. Asset Management

To ensure that security controls to protect the data and systems are applied effectively, Carlton Digby School will maintain asset registers for, files/systems that hold confidential data, and all physical devices (servers, switches, desktops, laptops etc) that make up its IT services.

6. User Accounts

Users are responsible for the security of their own accounts. If at any time they believe their credentials may have been compromised, for example after a phishing scam, they must change their password and inform IT Support as soon as possible. Personal accounts should not be used for work purposes. Carlton Digby School uses implement multi-factor authentication where it is practicable to do so.

7. Devices

To ensure the security of all Carlton Digby School issued devices and data, users are required to:

- Lock devices that are left unattended
- Update devices when prompted
- Report lost or stolen equipment as soon as possible to IT Support

- Change all account passwords at once when a device is lost or stolen (and report immediately to IT Support)
- Report a suspected threat or security weakness in Carlton Digby School’s systems to the Head Teacher or IT support

Devices will be configured with the following security controls as a minimum:

- Password protection
- Full disk encryption
- Client firewalls
- Anti-virus / malware software
- Automatic security updates
- Removal of unrequired and unsupported software
- Autorun disabled
- Minimal administrative accounts

8. Data Security

Carlton Digby School will take appropriate measures to reduce the likelihood of the loss of availability to, or the disclosure of, confidential data.

Carlton Digby School defines confidential data as:

- [Personally identifiable information](#) as defined by the ICO
- [Special Category personal data](#) as defined by the ICO
- Unpublished financial information

Critical data and systems will be backed up on a regular basis.

9. Sharing Files

Carlton Digby School recognises the security risks associated with sending and receiving confidential data.

To minimise the chances of a data breach users are required to:

- Consider if an email could be a phishing email or that a colleague’s account could be ‘hacked’. If something does not feel right check with the sender by another method, particularly in relation to financial transactions, attachments, or links to websites
- Wherever possible, keeping Carlton Digby School’s files on school systems / One Drive
- Not sending school files to personal accounts
- Verifying the recipient of data prior to sending
- Using file encryption where possible, sending passwords/keys via alternative communication channels
- Alerting IT Support / DPO to any breaches, malicious activity or suspected scams

10. Training

Carlton Digby School recognises that it is not possible to maintain a high level of Cybersecurity without appropriate staff training. It will integrate regular Cybersecurity training into Inset days, provide more specialist training to staff responsible for maintaining IT systems and promote a “No Blame” culture towards individuals who may fall victim to sophisticated scams.

11. System Security

IT Support will build security principles into the design of IT services for Carlton Digby School.

- Security patching – network hardware, operating systems and software
- Pro-actively plan for the replacement of network hardware, operating systems and software before vendors stop providing security support for them
- Actively manage anti-virus systems
- Actively manage and test backups
- Regularly review and update security controls that are available with existing systems
- Segregate wireless networks used for visitors' & staff personal devices from school systems
- Review the security risk of new systems or projects

12. Major Incident Response Plan

Carlton Digby School will develop, maintain, and regularly test a Cybersecurity Major Incident Response Plan (see separate document). This will include identifying or carrying out:

- Key decision-makers
- Key system impact assessments and restoration priorities (i.e. which backups needs to be restored first for the school to become operational again)
- Emergency plans for the school to function without access to systems or data
- Alternative methods of communication, including copies of contact details
- Emergency budgets and who can access them / how
- Key agencies for support (e.g. IT support company)




13. Maintaining Security

Carlton Digby School understands that the financial cost of recovering from a Major Cybersecurity Incident can far outweigh the ongoing investment in maintaining secure IT systems. Carlton Digby School will budget appropriately to keep cyber related risk to a minimum.

Appendix: Acceptable Use Policy Agreement





1. Pupils









? How to keep safe online






 Online means anything  connected to the  internet.

Most  devices and  apps are  connected to the  internet.










Devices are technology like  laptops,  game consoles,  tablets and  smart phones.










 I will only use the  devices  I am  allowed to use.








 I will  ask a  trusted  adult before  I use new  websites,  games or  apps.

 I will  ask for  help if  I am  stuck or not sure.







 I will be  kind and  polite to  everyone  online.

 I will  tell a  trusted  adult if  I feel  worried,  scared or  nervous when  online.






 I will  tell a  trusted  adult if  I feel  sad,  angry or  embarrassed when  online.










 I  will tell  a trusted  adult if  I  feel unsafe when using a  device.








 I  know people  online  sometimes  tell lies.

 They  might lie  about who they  are or where  they  live.

 I  never  have to keep  secrets from  my  trusted  adults.

 I  will not  change clothes or  undress in front of a  camera.

 I  will ask  a trusted  adult  before telling  anyone  my  information or  location.

 I  know that anything  I  do or  say  online  might be there forever.

It can be  given to my  family, my  friends or  strangers.

This could make  me  feel sad or  embarrassed.

 My  trusted  adults are _____.

 My  name is _____.

2. Staff and Governors

Background

All members of the Carlton Digby School community are required to electronically sign this Acceptable Use Policy (AUP), which sets out expectations for appropriate conduct when using technology, including:

- School networks, internet connections, devices, and cloud platforms
- Social media, both in and outside school

The AUP is reviewed annually and must be re-signed when updated or when a member of staff, governor, or volunteer joins the school.

All adults have legal and professional responsibilities to uphold the school's Online Safety, Safeguarding, and Curriculum commitments. Online safety is part of safeguarding and is everyone's responsibility.

Safeguarding and Reporting

- I recognise that online safety is part of safeguarding and forms part of my professional duty.
- I will report any concerns or breaches (by pupils or adults) immediately to the DSL or Head Teacher, following the Safeguarding and Child Protection Policy.
- I understand that safeguarding is a collective responsibility—my observations may complete a wider picture of concern.
- I will maintain a zero-tolerance approach to all forms of child-on-child abuse, including bullying and sexual harassment, and avoid victim-blaming language.

Professional Conduct

- I will model safe, responsible, and respectful online behaviour in all contexts, including social media.
- I will not post or share content that could bring the school or profession into disrepute, nor contact or accept contact from pupils through personal or social platforms.
- I will use school-approved systems (e.g. email, Class Dojo) for all professional communication.

Teaching and Supervision

- I will integrate online safety into everyday teaching and model positive digital behaviour.
- I will supervise pupils' use of technology, promote critical thinking, and check all online materials for accuracy, age-appropriateness, and suitability.
- I will report overblocking or attempts to bypass filtering to the DSL.
- During remote learning, I will follow the same safeguarding principles as when in school.

Use of School Systems and Devices

- I understand that all school systems are protected by filtering, monitoring, and security software, and that my use of devices, accounts, or logins (even off-site) may be monitored.
- I will not use school technology to access, store, or share material that is illegal, extremist, or inappropriate.
- I will care for devices loaned to me, use them safely, and never attempt to bypass school monitoring or security systems.

Data Protection and Cybersecurity

- I will adhere to the school's Data Protection and Cybersecurity Policies, on and off site.
- I will not store or share identifiable pupil or staff data on personal devices.

- I will immediately report any suspected data breach or cybersecurity incident.

Prevent Duty

- I will not support or promote extremist content, nor access, download, or share offensive or extremist material.

Commitment

- I understand that breaches of this AUP or the school's Online Safety Policy may lead to disciplinary action or referral to external agencies.
- I accept that it is my responsibility to remain informed and up to date with current safeguarding and online safety policies.

By electronically signing, I have read, understood and agreed to this policy and AUP. I understand that it is my responsibility to ensure I remain up to date and read and understand the school's most recent online safety and safeguarding policies. I understand that failure to comply with this agreement could lead to disciplinary action.