THE PERSE SCHOOL
CAMBRIDGE

Online Safety Policy

The Perse School

September 2026

Contents

1	Aims	1
2	Scope and application	1
3	Regulatory framework	1
4	Publication and availability	3
5	Definitions	3
6	Responsibility statement and allocation of tasks	4
7	Role of staff and parents	5
8	Filtering and monitoring	10
9	Access to the School's technology	11
10	Procedures for dealing with incidents of misuse	13
11	Education	15
12	Training	17
13	Cybercrime	20
14	Risk assessment	21
15	Record keeping	22
16	Version control	22

1 Aims

1.1 This is the Online Safety Policy of The Perse School (**the School**). The School comprises the **Relevant Schools** (the Perse Pelican Nursery and Pre Preparatory School including the EYFS setting (**Pelican School**), the Perse Preparatory School (**Prep School**) and the Perse Upper School (**Upper School**)).

1.2 The aim of this policy is to promote and safeguard the welfare of all pupils through the implementation of an effective online safety strategy which empowers the School to:

1.2.1 protect the whole School community from potentially illegal, inappropriate and harmful content or contact;

1.2.2 educate the whole School community about their access to and use of technology;

1.2.3 establish effective mechanisms to identify, intervene in and escalate concerns where appropriate; and

1.2.4 help to promote a whole school culture of openness, safety, equality and protection.

1.3 This policy forms part of the School's whole school approach to promoting child safeguarding and wellbeing, which involves everyone at the School and seeks to ensure that the best interests of pupils underpins and is at the forefront of all decisions, systems, processes and policies.

1.4 Online safety is a running and interrelated theme throughout the devising and implementation of many of the School's policies and procedures (including its Safeguarding and Child Protection Policy and Procedures) and careful consideration has been given to ensure that it is also reflected in the School's curriculum, teacher training and any parental engagement, as well as the role and responsibility of the School's Designated Safeguarding Lead (DSL) and any deputies.

1.5 Although this policy is necessarily detailed, it is important to the School that our safeguarding related policies and procedures are transparent, clear and easy to understand for staff, pupils, parents and carers. The School welcomes feedback on how we can continue to improve our policies.

2 Scope and application

2.1 This policy applies to the whole School including the Early Years Foundation Stage (**EYFS**).

2.2 This policy applies to all members of the School community, including staff and volunteers, pupils, parents and visitors, who have access to the School's technology whether on or off School premises, or otherwise use technology in a way which affects the welfare of other pupils or any member of the School community or where the culture or reputation of the School is put at risk.

3 Regulatory framework

3.1 This policy has been prepared to meet the School's responsibilities under:

3.1.1 Education (Independent School Standards) Regulations 2014;

3.1.2 Early years foundation stage statutory framework For group and school-based providers (DfE, September 2026) and the Children Act 1989;

3.1.3 Education and Skills Act 2008;

3.1.4 Childcare Act 2006;

3.1.5 Data Protection Act 2018 and UK General Data Protection Regulation (UK GDPR) and the Data (Use and Access) Act 2025 (together referred to as "data protection laws"); and

3.1.6 Equality Act 2010.

3.2 This policy has regard to the following guidance and advice:

3.2.1 Keeping children safe in education (DfE, September 2026) (KCISIE);

3.2.2 Preventing and tackling bullying (DfE, July 2017);

3.2.3 Sharing nudes and semi-nudes: advice for education settings working with children and young people (Department for Science, Innovation & Technology (DSIT) and UK Council for Internet Safety (UKCIS), March 2024);

3.2.4 Prevent duty guidance: for England and Wales (Home Office, October 2023, updated March 2024);

3.2.5 Channel duty guidance: protecting people susceptible to radicalisation (Home Office, October 2023, updated October 2025).

3.2.6 Relationships Education, Relationships and Sex Education (RSE) and Health Education guidance (DfE, DfE July 2025 and effective from 1 September 2026);

3.2.7 Searching, screening and confiscation: advice for headteachers, school staff and governing bodies (DfE, July 2022, in force from September 2022);

3.2.8 Safeguarding children and protecting professionals in early years settings; online safety considerations (UKCIS, February 2019);

3.2.9 Help for early years providers: Screen use (DfE, July 2026)

3.2.10 Behaviour in schools: advice for headteachers and school staff (DfE, February 2024);

3.2.11 Mobile phones in schools (DfE, January 2026, became statutory on 29 June 2026);

3.2.12 Teaching online safety in schools (DfE, January 2023);

3.2.13 Harmful online challenges and online hoaxes (DfE, February 2021);

3.2.14 Online safety guidance if you own or manage an online platform (DSIT, June 2021);

3.2.15 A business guide for protecting children on your online platform (DSIT, June 2021);

3.2.16 Online safety audit tool (UKCIS, October 2022);

3.2.17 Meeting digital and technology standards in education (DfE, January 2024);

3.2.18 Appropriate filtering for education settings (UKSIC, May 2025);

3.2.19 Online Safety Self-Review Tool for Schools, 360safe; and

3.2.20 Appropriate monitoring for schools (UKSIC, May 2026); and

3.2.21 Online safety in schools and colleges: questions from the governing board (UKCIS, October 2022);

3.2.22 Plan technology for your school (HM Government, November 2025);

3.2.23 Generative artificial intelligence (AI) in education (DfE, updated August 2025);

3.2.24 Generative AI; product safety expectations (DfE, January 2026); and

3.2.25 Using AI in education settings: support materials (DfE, updated May 2026).

3.3 The following School policies, procedures and resource materials are relevant to this policy:

3.3.1 Acceptable Use of ICT Policy for Pupils;

3.3.2 Acceptable Use of ICT Policy for Staff and Social Media Policy;

3.3.3 Safeguarding and Child Protection Policy;

3.3.4 Anti-Bullying Policy (Pupils);

3.3.5 Behaviour and Discipline Policy;

3.3.6 Risk Assessment Policy for Pupil Welfare;

3.3.7 Staff Code of Conduct and Whistleblowing Policy;

3.3.8 Data Protection Policy;

3.3.9 Relationships Education and Relationships and Sex Education policy;

3.3.10 Information Security and Sharing Data Guidance; and

4 Publication and availability

4.1 This policy is published on the School website.

4.2 This policy is available in hard copy on request.

4.3 A copy of the policy is available for inspection from the school office during the School day.

4.4 This policy can be made available in large print or other accessible format if required.

5 Definitions

5.1 Where the following words or phrases are used in this policy:

5.1.1 References to **Designated Safeguarding Lead** (DSL) are references to the Designated Safeguarding Lead for the Relevant School.

5.1.2 References to **Online Safety Lead** are references to the Online Safety Lead for the Relevant School (as identified in the Key School Contacts section of the School's Safeguarding and Child Protection Policy) who assist the DSL in discharging their duties under KCSIE (see paragraph 7.1 below). The online safety leads are:

(a) Pelican School - Tim Ankin (Deputy Head), teankin@perse.co.uk;

(b) Prep School – Tobias Bown (Assistant Head (Academic)), tabown@perse.co.uk; and

(c) Upper School – Amy Cockerill (Assistant Head (Safeguarding)), arcockerill@perse.co.uk.

5.1.3 References to the **Proprietor** are references to the Board of Governors.

5.1.4 References to **staff** includes all those who work for or on behalf of the School, regardless of their employment status, including supply staff, contractors, volunteers and Governors unless otherwise indicated.

5.1.5 **Senior Leadership Team** (**SLT**) comprises of the Upper School Executive Leadership Team, the Prep School Senior Management Team and the Pelican School Senior Leadership Team.

5.1.6 The term **"making or sharing nudes and semi-nudes"** refers to the creation, sending or posting of nude or semi-nude images by young people under the age of 18. The term **"images"** includes all visual content, such as photographs, videos and livestreams. Images may be taken by the child themselves or taken or created by another person. They may also be digitally altered or wholly generated using artificial intelligence, including what are sometimes described as "deepfakes" or "deep nudes".

5.1.7 In considering the scope of the School's online safety strategy, the School will take a wide and purposive approach to considering what falls within the meaning of technology, networks and devices used for viewing or exchanging information (collectively referred to in this policy as **technology**).

6 Responsibility statement and allocation of tasks

6.1 The Board of Governors has overall responsibility for all matters which are the subject of this policy and for approving and reviewing its effectiveness.

6.2 The Board of Governors is required to ensure that all those with leadership and management responsibilities at the School actively promote the well-being of pupils. The adoption of this policy is part of the Proprietor's response to this duty.

6.3 To ensure the efficient discharge of its responsibilities under this policy, the Board of Governors has allocated the following tasks:

Task	Allocated to	When / frequency of review
Keeping the policy up to date and compliant with the law and best practice	Upper School - Deputy Head (Pupil development and welfare) Prep School – Deputy Head Pelican School – Deputy Head	As required, and at least annually
Monitoring the implementation of the policy, including the record of	Upper School - Deputy Head (Pupil development and welfare)	As required, and at least termly

Task	Allocated to	When / frequency of review
incidents involving the use of technology and the logs of internet activity and sites visited, relevant risk assessments and any action taken in response and evaluating effectiveness	Prep School – Deputy Head Pelican School – Deputy Head	
The School's approach to Online safety	Designated Safeguarding Lead	As required, and at least annually
Reviewing digital technology strategy	Online Safety Leads	As required, and at least annually
Taking appropriate action to meet the Cyber security standards for schools and colleges[1]	Online Safety Leads	As required, and at least annually
Seeking input from interested groups (such as pupils, staff, Parents) to consider improvements to the School's processes under the policy	Upper School - Deputy Head (Pupil development and welfare) Prep School – Deputy Head Pelican School – Deputy Head	As required, and at least annually
Assessing the School's approach to filtering and monitoring and accessing this in light of new or emerging risks and technologies	Designated Safeguarding Leads Senior Leadership Team Director of ICT Nominated Safeguarding Governor (see the School's Safeguarding and Child Protection Policy Key School Contacts section)	As required, and at least annually
Formal annual review	Board of Governors	Annually

7 Role of staff and parents

7.1 Head and Senior Leadership Team

7.1.1 The Head has overall executive responsibility for the safety and welfare of members of the School community. This includes a specific responsibility to ensure that the

[1] The Cyber security standards for schools and colleges were developed to help schools improve their resilience against cyber-attacks. Broader guidance on cyber security including considerations for governors and trustees can be found at National Cyber Security Centre - NSCC.

School has an effective filtering policy in place and that it is applied and updated on a regular basis.

7.1.2 The Designated Safeguarding Lead is the senior member of staff from the School's leadership team with lead responsibility for safeguarding and child protection, including online safety and understanding the filtering and monitoring systems in place in school.

(a) The responsibility of the Designated Safeguarding Lead includes;

(i) managing safeguarding incidents involving the use of technology (including through the use of generative AI) in the same way as other safeguarding matters, in accordance with the School's Safeguarding and Child Protection Policy;

(ii) Working with the Online Safety Lead to ensure all staff are appropriately trained and aware of the procedures that need to be followed in the event of an online safety incident taking place and the need to immediately report those incidents;

(iii) Working with the Director of ICT (see below) and Online Safety Lead in monitoring technology uses (including through the use of generative AI) and practices across the School and assessing whether any improvements can be made to ensure the online safety and well-being of pupils.

(iv) Overseeing and acting on filtering and monitoring reports, safeguarding concerns and checks to filtering and monitoring systems;

(v) Overseeing and acting on: arrangements for information and cyber security and action taken to meet the Cyber security standards to protect the School from cyber-attacks and improve cyber resilience;

(vi) Regularly monitoring the technology incident log maintained by the Director of ICT and working with the Online Safety Lead to assess whether changes need to be made to the digital technology strategy and staff and pupil training;

(vii) Regularly updating other members of the School's Senior Leadership Team and the Governors on the operation of the School's safeguarding arrangements, including online safety practices;

(viii) Providing online safety training and advice to governors, staff, parents, carers and pupils including on online harms and how to identify illegal, harmful or inappropriate content, including content created or accessed through the use of generative AI; and

(ix) Promoting an awareness of and commitment to online safety education / awareness raising across the School and beyond.

7.2 **Online Safety Lead**

7.2.1 The Online Safety Lead is a member of the senior leadership team and the safeguarding team.

7.2.2 The Head of Computing and Digital Strategy works closely with the Director of ICT and the Online Safety Lead. They have strategic oversight of all digital technology for teaching and learning. They will create and manage the digital technology strategy led by the needs of staff and students.

7.2.3 The Head of Computing and Digital Strategy will be accountable for:

(a) the delivery of the digital technology strategy based on teaching and learning outcomes and organisational needs;

(b) encouraging and supporting the use of digital technology (including through the use of generative AI) across the school;

(c) reviewing the effectiveness of IT support to inform decision making and taking action, when necessary;

(d) identifying and acting on digital technology training needs for staff and students;

(e) organising and chairing regular ICT strategy, 3-18 online safety & Upper Online Safety meetings.

7.3 **Director of ICT**

7.3.1 The Director of ICT together with their team, is responsible for the effective operation of the School's filtering and monitoring systems so that pupils and staff are unable to access any material that poses a safeguarding risk, including terrorist and extremist material, while using the School's network.

7.3.2 The Director of ICT is responsible for ensuring that:

(a) the user may only use the School's technology if they are properly authenticated and authorised;

(b) the risks of pupils and staff circumventing the safeguards put in place by the School are minimised;

(c) the use of the School's technology is regularly monitored to ensure compliance with this policy and that any misuse or attempted misuse can be identified and reported to the appropriate person for investigation; and

(d) monitoring software and systems are kept up to date to allow the IT team to monitor the use of email and the internet over the School's network and maintain logs of such usage.

(e) reviewing the effectiveness of IT support to inform decision making and taking action, when necessary;

(f) identify any potential compromises to safeguarding or risk of a cyber-attack;

(g) overseeing the effectiveness and appropriateness of the School's filtering and monitoring systems, having regard to the School's context, and ensuring that records are kept of checks undertaken;

(h) reviewing registers relating to hardware and systems to ensure they are up to date;

(i) reviewing measures in place on the School's use of generative AI and measures taken to combat cybercrime;

(j) carrying out reviews of filtering and monitoring systems, at least once every academic year, to ensure their effectiveness. See Section 8 below;

(k) proactively identify any potential compromises to safeguarding or risk of a cyber-attack to ensure compliance with the Cyber security standards;

(l) ensuring digital technology is included within insurance arrangements and disaster recovery and business continuity plans; and

7.3.3 Appendix 3 of the Acceptable Use of ICT Policy for Staff outlines the School's Technical Infrastructure and Reporting Mechanisms. In summary:

(a) Using a software application, the school monitors all essential hardware and software services. Email alerts are sent to senior IT staff 24/7 alerting them of problems and potential problems on the network.

(b) The Director of ICT reports to the Senior Bursary Team and Executive Leadership Team regularly.

(c) The Director of ICT receives daily emails from web filtering software listing users who have visited inappropriate sites or tried to download inappropriate content. The Director of ICT will escalate concerns to the DSL if necessary.

7.3.4 The Director of ICT will report regularly to the Senior Leadership Team on the operation of the School's technology. If the Director of ICT has concerns about the functionality, effectiveness, appropriateness or use of technology within the School, including the monitoring and filtering systems in place, they will escalate those concerns promptly to the Designated Safeguarding Lead.

7.3.5 The Director of ICT is responsible for maintaining the technology incident log (a central record of all serious incidents involving the use of technology) and bringing any matters of safeguarding concern to the attention of the Designated Safeguarding Lead in accordance with the School's Safeguarding and Child Protection Policy.

7.4 **All staff**

7.4.1 All staff are expected to adhere, so far as applicable, to each of the policies referenced in this policy.

7.4.2 Training of all staff includes online safety which, amongst other things, includes an understanding of filtering and monitoring provisions in place, how to manage them effectively, the use of generative AI and the risks associated with this, how to escalate concerns when identified and any particular expectations or responsibilities in relation to filtering and monitoring.

7.4.3 All staff have a responsibility to act as good role models in their use of technology and to share their knowledge of the School's policies and of safe practice with the pupils.

7.4.4 Staff should follow the guidance covering the use of technology in the classroom which is contained in Appendix 2 of the Acceptable Use of IT Policy for Staff.

7.4.5 All staff are aware that technology (including the use of generative AI) can play a significant part in many safeguarding and wellbeing issues and that pupils are at risk of abuse online as well as face-to-face. Staff are also aware that, sometimes, such abuse will take place concurrently online and during a pupil's daily life.

7.4.6 Staff are expected to be alert to the possibility of pupils abusing their peers online and to understand that this can occur both inside and outside of school. Examples of such abuse can include:

(a) the sending of abusive, harassing and misogynistic messages;

(b) the consensual and non-consensual making or sharing of nudes and semi-nudes (especially around group chats);

(c) the sharing of abusive images and pornography to those who do not wish to receive such content; and/or

(d) cyberbullying,

7.4.7 Staff are also aware that many other forms of abuse may include an online element. For instance, there may be an online element which:

(a) facilitates, threatens and/or encourages physical abuse;

(b) facilitates, threatens and/or encourages sexual violence; or

(c) is used as part of initiation/hazing type violence and rituals.

7.4.8 It is important that staff recognise the indicators and signs of child-on-child abuse, including where such abuse takes place online, and that they know how to identify it and respond to reports. Staff must also understand that, even if there are no reports of child-on-child abuse at the School, whether online or otherwise, it does not mean that it is not happening; it may simply be the case that it is not being reported.

7.4.9 It is important that staff challenge inappropriate behaviours between peers and do not downplay certain behaviours, including harmful sexual behaviour, sexual violence and sexual harassment, as "*just banter*", "*just having a laugh*", "*part of growing up*" or "*boys being boys*" as doing so can result in a culture of unacceptable behaviour, misogyny, misandry, an unsafe environment for children and, in a worst case scenario, a culture that normalises abuse leading to children accepting it as normal and not coming forward. The School has a **zero-tolerance approach** towards child-on-child abuse (including in relation to harmful sexual behaviour, sexual violence and sexual harassment) and such behaviour is never acceptable and will not be tolerated. The School will treat any such incidences as a breach of discipline and will deal with them under the School's Behaviour and Discipline Policy and also as a safeguarding matter under the School's Safeguarding and Child Protection Policy and procedures.

7.4.10 Staff have a responsibility to report any concerns about a pupil's welfare and safety in accordance with this policy and the School's Safeguarding and Child Protection Policy. If staff have any concerns regarding child-on-child abuse or if they are unsure as to how to proceed in relation to a particular incident, they should **always speak to the Designated Safeguarding Lead in all cases.**

7.5 **Parents**

7.5.1 The role of parents in ensuring that pupils understand how to stay safe when using technology is crucial. The School expects parents to promote safe practice when using technology and to:

(a) support the School in the implementation of this policy and report any concerns in line with the School's policies and procedures;

(b) talk to their child to understand the ways in which they are using the internet, social media and their mobile devices and promote responsible behaviour;

(c) encourage their child to speak to someone if they are being bullied or otherwise are concerned about their own safety or that of another pupil or need support; and

(d) support the School's policy on prohibiting the use of mobile phones.

7.5.2 If parents have any concerns or require any information about online safety, they should contact the Designated Safeguarding Lead. They can also consult the online safety resources detailed in section 12.3.6.

8 Filtering and monitoring

8.1 Whilst considering their responsibility to safeguard and promote the welfare of pupils and provide them with a safe environment in which to learn, the Board of Governors will do all it reasonably can to limit pupils' exposure to risks from the School's IT system. As part of this process, the School has appropriate filtering and monitoring systems in place and the Board of Governors ensures that a review of their effectiveness is carried out at least once every academic year.

8.2 The School has regard to Government filtering and monitoring standards, which require that the School;

8.2.1 Identifies and assigns roles and responsibilities to manage filtering and monitoring systems;

8.2.2 Has effective monitoring strategies in place that meet their safeguarding needs;

8.2.3 Blocks harmful and inappropriate content without unreasonably impacting teaching and learning; and

8.2.4 Reviews filtering and monitoring provision and its effectiveness at least annually.

8.3 The Director of ICT ensures that the senior leadership team and relevant staff have an awareness and understanding of the filtering and monitoring provisions in place, manage them effectively and know how to escalate concerns when identified.

8.4 In carrying out their checks, the Director of ICT ensures that filtering is working appropriately on all internet-connected devices in all relevant locations, and a record is kept of these checks.

8.5 The School will assess its approach to filtering and monitoring to reflect the risks it faces and will continue to assess this in light of new or emerging risks and technologies.[2]

8.6 The School manages access and restrictions to content across its systems for all users, including guest accounts. Logs / alerts are regularly reviewed and acted upon.

8.7 The School has provided enhanced/differentiated user-level filtering (allowing different filtering levels for different abilities/ages/stages and different groups of users: staff/pupils, etc. Younger learners use child friendly / age-appropriate search engines e.g. SWGfL Swiggle.

8.8 The School understands the extent to which content is dynamically analysed where it is streamed in real-time (including content created by users or through generative AI) to the user and blocked.

8.9 Access to content through non-browser services e.g. apps and other mobile technologies is managed in ways that are consistent with this policy.

8.10 The School has monitoring systems in place to protect the School, systems and users. It monitors all network use across all its devices and services. Logs/alerts are regularly reviewed and acted upon.

8.11 The School uses a number of monitoring strategies to minimise safeguarding risks on internet connected devices, including;

8.11.1 Physical monitoring by staff watching screens of users;

8.11.2 Live supervision by staff on a console with device management software;

8.11.3 Network monitoring using log files of internet traffic and web access; and

8.11.4 Individual device monitoring through software or third-party services.

9 Access to the School's technology

9.1 The School provides internet, intranet access and an email system to pupils and staff as well as other technology. Pupils and staff must comply with the respective *Acceptable Use of ICT Policy* when using School technology. All such use is monitored by the IT department.

9.2 Pupils and staff require individual usernames and passwords to access the School's internet, intranet and email system which must not be disclosed to any other person. Any pupil or member of staff who has a problem with their usernames or passwords must report it to the IT department immediately.

9.3 The use of any personal device connected to the School's network will be logged and monitored by the IT Department. Appropriate use of the School's network is covered within the acceptable use of ICT policy for pupils. When connecting devices to the School's Wi-Fi, pupils and staff sign in using their school credentials. Individualised visitor guest Wi-Fi codes are issued allowing the School to monitor any unusual network traffic. See also 9.5 below and the School's information security and sharing data guidance for staff (including remote working and bringing your own device to work).

[2] See 'Plan technology for your school' (HM Government, November 2025) which includes a self-assessment tool to assist schools in meeting the filtering and monitoring standards.

9.4 The School has a separate wireless network connection available for use by visitors to the School. Individual guest wireless network codes are available from the IT Department and will only be valid for a short amount of time. Use of this service will be logged and monitored by the IT Department. The Sports Centre has a separate guest Wi-Fi network where visitors need to register their details before accessing the School's Wi-Fi network.

9.5 **Inappropriate material**

9.5.1 The School recognises the importance of ensuring that all pupils are safeguarded from potentially harmful and inappropriate material online.

9.5.2 Online safety is a key element of many school policies and procedures and an important part of the role and responsibilities of the Designated Safeguarding Lead. The term 'online safety' encapsulates a wide range of ever evolving issues, but these can be classified into four main areas of risk:

(a) **Content** - being exposed to illegal, inappropriate or harmful content, including for example: pornography, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism, extreme sexual or physical violence, misinformation, disinformation (including fake news) and conspiracy theories;

(b) **Contact** - being subjected to harmful online interaction with other users or generative AI applications that simulate this (e.g. peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom and/or exploit them for sexual, criminal, financial or other purposes);

(c) **Conduct** - a pupil's personal online behaviour that increases the likelihood of, or causes, harm (e.g. making, sending and receiving explicit images (such as the consensual and non-consensual making or sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and

(d) **Commerce** - risks such as online gambling, inappropriate advertising, phishing and / or financial scams. If pupils, students or staff are at risk, it should be reported to the Anti-Phishing Working Group.

9.6 **Use of mobile electronic devices and smart technology**

9.6.1 In accordance with DfE guidance, the School maintains a mobile electronic device-free environment for pupils by default[3]. For detailed information of the use of mobile electronic devices and smart technology, please refer to the School's Acceptable Use of ICT Policy for Pupils.

[3] Section 36 of the Children's Wellbeing and Schools Act 2026 requires schools in England to have regard to published guidance on mobile phones. This gives the guidance on mobile phones in schools the force of law. The provision came into force on 29 June 2026. Schools must implement a policy whereby pupils do not have access to their mobile phone throughout the school day including lessons, the time between lessons, breaktimes and lunchtime. There are a number of ways in which schools can ensure that they are mobile phone-free, and it is for headteachers to decide how best to achieve this within their own unique contexts.

10 Procedures for dealing with incidents of misuse

10.1 Staff, pupils and parents are required to report incidents of misuse or suspected misuse to the School in accordance with this policy and the School's safeguarding and disciplinary policies and procedures.

10.2 The School recognises the importance of acknowledging, understanding and not downplaying behaviours which may be related to abuse and has appropriate systems in place to ensure that pupils can report any incidents of abuse, whether or not they include an online element, confidently and safe in the knowledge that their concerns will be treated seriously. Staff should however be careful not to promise that a concern will be dealt with confidentially at an early stage as information may need to be shared further (e.g. with the Designated Safeguarding Lead) to discuss next steps. Teaching is tailored to the specific needs and vulnerabilities of individual children, such as those who are victims of abuse, children with SEN or disabilities.

10.3 **Misuse by pupils**

10.3.1 Anyone who has any concern about the misuse of technology by pupils should report it immediately so that it can be dealt with in accordance with the School's behaviour and discipline policies, including the Anti-Bullying Policy where there is an allegation of cyberbullying.

Type of misuse	Relevant policy	Reporting channel
Bullying	Anti-bullying	Form Tutor / teacher or trusted member of staff.
Sexual violence, harmful sexual behaviour and sexual harassment (whether during or outside of school)	Safeguarding and Child Protection Policy	The DSL, who has overall responsibility for online safety matters
Consensual and non-consensual making or sharing of nudes and semi-nudes	Safeguarding and Child Protection Policy	Form Tutor / teacher or trusted member of staff. Who should then refer to the DSL who has overall responsibility for safeguarding including online safety matters
Harassment	Safeguarding and Child Protection Policy	
Upskirting	Safeguarding and Child Protection Policy	
Radicalisation	Safeguarding and Child Protection Policy	

Type of misuse	Relevant policy	Reporting channel
Other breach of acceptable use policy, including unauthorised use of mobile devices.	See relevant policy referred to in acceptable use policy	Form Tutor / teacher or trusted member of staff. Note any incidents which give rise to safeguarding concerns must be referred on to the Designated Safeguarding Lead
Any action resulting in disruption to digital technology systems in school	Digital technology strategy	Online Safety Lead Note any incidents which give rise to safeguarding concerns must be referred on to the Designated Safeguarding Lead

10.3.2 Anyone who has any concern about the welfare and safety of a pupil must report it immediately in accordance with the School's child protection procedures (see the School's Safeguarding and Child Protection Policy).

10.4 **Misuse by staff**

10.4.1 Anyone who has any concern about the misuse of technology by staff should report it in accordance with the School's Whistleblowing Policy so that it can be dealt with in accordance with the staff disciplinary procedures.

10.4.2 If anyone has a safeguarding-related concern relating to staff misuse of technology, they must report it immediately in accordance with the School's policy on raising concerns and dealing with allegations which is set out in the School's Safeguarding and Child Protection Policy.

10.4.3 Anyone who has any other concern about the misuse of technology by staff should report their concerns as set out below:

(a) Staff should speak to their senior line manager in the Executive Leadership Team (Upper) or Senior Bursary Team or the Deputy Head or Head (Prep and Pelican School) in accordance with the School's *Whistleblowing Policy*; and

(b) Anyone else should speak to the Head.

10.5 **Misuse by any user**

10.5.1 Anyone who has any concern about the misuse of technology by any other user should report it immediately to the Director of ICT, the Designated Safeguarding Lead, the Bursar or the Head.

10.5.2 The School reserves the right to withdraw access to the School's network by any user at any time and to report suspected illegal activity to the police.

10.5.3 If the School considers that any person is vulnerable to radicalisation the School will refer this to the Channel programme. This focuses on support at an early stage to people who are identified as being vulnerable to being drawn into terrorism. Any person who has a concern relating to extremism may report it directly to the police.

11 Education

11.1 The teaching of online safety is integrated, aligned and considered as part of the whole school safeguarding approach and wider staff training and curriculum planning.

11.2 The School ensures that children are taught how to keep themselves and others safe, including online, and the safe use of technology and use of generative AI tools is therefore integral to the School's curriculum. Pupils are educated in an age-appropriate manner about the importance of safe and responsible use of technology, including the internet, social media and mobile electronic devices and on the use of generative AI tools (see the School's curriculum policy). Teaching is tailored to the specific needs and vulnerabilities of individual children, such as those who are victims of abuse, children with SEN or disabilities.

11.3 Technology is included in the educational programmes followed in the EYFS in the following ways:

11.3.1 children are guided to make sense of their physical world and their community through opportunities to explore, observe and find out about people, places, technology and the environment;

11.3.2 children are enabled to explore and play with a wide range of media and materials and provided with opportunities and encouragement for sharing their thoughts, ideas and feelings through a variety of activities in art, music, movement, dance, role-play, and design and technology; and

11.3.3 children are guided to recognise that a range of technology is used in places such as homes and schools and encouraged to select and use technology for particular purposes.

11.4 The safe use of technology is also a focus in all areas of the curriculum and teacher training and key safety messages are reinforced as part of assemblies, PSHE and tutorial / pastoral activities, teaching pupils:

11.4.1 about the risks associated with using the technology (including through generative AI) and how to protect themselves and their peers from potential risks;

11.4.2 about the importance of identifying, addressing and reporting inappropriate behaviour, whether on or offline, and the risks of downplaying such behaviour as, for example, "banter" or "just boys being boys";

11.4.3 to be critically aware of content they access online (including how to recognise illegal, inappropriate or harmful content) and guided to validate accuracy of information;

11.4.4 to be aware of and how to identify the risks posed by cybercrime

11.4.5 how to recognise suspicious, bullying or extremist behaviour;

11.4.6 the definition of cyberbullying, its effects on the victim and how to treat each other's online identities with respect;

11.4.7 relevant laws applicable to the internet

11.4.8 the consequences of negative online behaviour;

11.4.9 Understanding the risks of bias or misleading information that can be produced by automated and AI generated content;

11.4.10 how to report cyberbullying and / or incidents that make pupils feel uncomfortable or under threat and how the School will deal with those who behave badly; and

11.4.11 how to respond to harmful online challenges and hoaxes.

11.5 The School recognises the crucial role it plays in relation to preventative education and that this is most effective in the context of a whole school approach that prepares pupils for a life in modern Britain and creates a culture of zero tolerance for sexism, racism, misogyny/misandry, homophobia, biphobia, child-on-child abuse including and sexual violence and sexual harassment derogatory behaviour and other forms of physical violence and conflict.

11.6 Pupils are also taught about the risks associated with all forms of abuse, including physical abuse and sexual violence and sexual harassment which may include an online element. The School has a zero-tolerance approach to harmful sexual behaviour, sexual violence and sexual harassment, and such behaviour is never acceptable and will not be tolerated. The School will treat any such incidences as a breach of discipline and will deal with them under the School's Behaviour and Discipline Policy and also as a safeguarding matter under the School's Safeguarding and Child Protection Policy and procedures.

11.7 The safe use of technology aspects of the curriculum are reviewed on a regular basis to ensure their relevance.

11.8 The School's Acceptable Use of ICT Policy for Pupils sets out the School rules about the use technology including internet, email, social media and mobile electronic devices, helping pupils to protect themselves and others when using technology. Pupils are reminded of the importance of this policy on a regular basis.

11.9 The School recognises that effective education needs to be tailored to the specific needs and vulnerabilities of individual pupils, including those who are victims of abuse, and those with special educational needs and disabilities, and this is taken into account when devising and implementing processes and procedures to ensure the online safety of its pupils. For more details on the School's approach, the School's Safeguarding and Child Protection Policy and its Relationships Education and RSE Policy.

11.10 **Useful online safety resources for pupils**

11.10.1 https://www.thinkuknow.co.uk/

11.10.2 https://www.childnet.com/resources/smartie-the-penguin/

11.10.3 https://www.childnet.com/resources/digiduck-stories/

11.10.4 http://www.childnet.com/young-people

11.10.5 https://www.saferinternet.org.uk/advice-centre/young-people

11.10.6 https://mysafetynet.org.uk/

11.10.7 https://www.ceop.police.uk/Safety-Centre/How-can-CEOP-help-me-YP/

11.10.8 https://www.bbc.com/ownit

12 Training

12.1 Proprietor

12.1.1 To ensure that all Governors and Trustees are equipped with the knowledge to provide strategic challenge to test and assure themselves that the safeguarding policies and procedures of the School are effective and that they support the delivery of a robust whole school approach to safeguarding, all Governors and Trustees receive appropriate safeguarding and child protection (including online safety) training at induction. This training is regularly updated.

12.2 Staff

12.2.1 The School provides training on the safe use of technology to staff so that they are aware of how to protect pupils and themselves from the risks of using technology and to deal appropriately with incidents involving the use of technology when they occur.

12.2.2 Induction training for new staff includes training on the School's online safety strategy including this policy, the *Code of Conduct for Staff* and *Acceptable Use of ICT Policy for Staff*. Staff training is regularly updated, and ongoing staff development training includes (but is not limited to) training on technology safety together with specific safeguarding issues including the consensual and non-consensual making or sharing of nudes and semi-nudes, cyberbullying, radicalisation, dealing with harmful online challenges and online hoaxes and on the risks associated with generative AI tools and content created by them. This training may be in addition to the regular safeguarding and child protection (including online safety) training as required at induction and at least annually thereafter. Training specifically addresses the School's filtering and monitoring provisions in place, including activity logging and reporting mechanisms and how to manage them effectively, how to escalate concerns when identified and any particular staff expectations or responsibilities including on the use of approved generative AI tools for educational purposes.

12.2.3 Where pupils wish to report a safeguarding concern, all staff are taught to reassure victims that they are being taken seriously and that they will be supported and kept safe. Staff are aware of the importance of their role in dealing with safeguarding and

wellbeing issues, including those involving the use of technology, and understand that a victim should never be given the impression that they are creating a problem by reporting abuse, including harmful sexual behaviour, sexual violence or sexual harassment, and nor should they ever be made to feel ashamed for making a report.

12.2.4 Where safeguarding incidents involve an online element, such as the making or sharing of nudes and semi-nudes, staff will not view or forward images reported to them and will follow the School's policy on the consensual and non-consensual making or sharing of nudes and semi-nudes as set out in The School's *Safeguarding and Child Protection Policy* and Searching, screening and confiscation: advice for schools. In certain cases, it may be appropriate for staff to confiscate a pupil's devices to preserve any evidence and hand it to the police for inspection.

12.2.5 Staff are encouraged to adopt and maintain an attitude of 'it could happen here' where safeguarding is concerned, including in relation to harmful sexual behaviour, sexual violence and sexual harassment and to address inappropriate behaviours (even where such behaviour appears relatively innocuous) as this can be an important means of intervention to help prevent problematic, abusive and/or violent behaviour in the future

12.2.6 Staff are trained to recognise any illegal, inappropriate or harmful content, including content created through generative AI tools, and to look out for potential patterns of concerning, problematic or inappropriate behaviour and, where a pattern is identified, the School will decide on an appropriate course of action to take. Consideration will also be given as to whether there are wider cultural issues within the School that facilitated the occurrence of the inappropriate behaviour and, where appropriate, extra teaching time and/or staff training will be delivered to minimise the risk of it happening again.

12.2.7 Staff also receive data protection training on induction and at regular intervals afterwards.

12.2.8 The frequency, level and focus of all such training will depend on individual roles and requirements and will be provided as part of the School's overarching approach to safeguarding.

12.2.9 **Useful online safety resources for staff**

(a) https://www.saferinternet.org.uk/advice-centre/teachers-and-professionals

(b) http://www.childnet.com/teachers-and-professionals

(c) https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online-safety/

(d) https://www.thinkuknow.co.uk/teachers/

(e) http://educateagainsthate.com/

(f) https://www.commonsense.org/education/

(g) Cyberbullying: advice for head teachers and school staff (DfE, November 2014)

(h) Advice on the use of social media for online radicalisation (DfE and Home Office, July 2015)

(i) Sharing nudes and semi-nudes: advice for education settings working with children and young people (DSIT and UKCIS, March 2024)

(j) Online safety in schools and colleges: questions from the governing board (UKCIS, October 2022)

(k) Understanding and responding to AI-generated child sexual abuse material (National Crime Agency's CEOP Education, June 2026)

(l) Financially motivated sexual extortion: alert for education settings (National Crime Agency's CEOP Education)

(m) Using External Expertise to Enhance Online Safety Education(UKCIS, October 2022)

(n) Education for a connected world framework (UKCIS, June2020)

(o) Online Sexual Harassment: Understand, Prevent and Respond Guidance for Schools (Childnet, March 2019)

(p) Myth vs Reality: PSHE toolkit (Childnet, April 2019)

(q) SELMA Hack online hate toolkit (SWGFL, May 2019)

(r) Teaching online safety in school: Guidance supporting schools to teach their pupils how to stay safe online, within new and existing school subjects (DfE, January 2023)

(s) Harmful online challenges and online hoaxes (DfE, February 2021)

(t) Professionals online safety helpline: helpline@saferinternet.org.uk, 0344 381 4772

(u) NSPCC helpline for anyone worried about a child - 0808 800 5000

(v) Internet Watch Foundation - internet hotline for the public and IT professionals to report potentially criminal online content

(w) https://lgfl.net/safeguarding/resources

12.2.10 The Cambridgeshire and Peterborough Safeguarding Partnership has produced guidance on radicalisation which is available here:

https://safeguardingcambspeterborough.org.uk/childrenboard/professionals/prevent/.

12.3 **Parents**

12.3.1 The School is in regular contact with parents and carers and uses communications to reinforce the importance of ensuring that children are safe online. The School aims to help parents understand what systems are in place to filter and monitor their child's online use and ensures that parents are aware of what their children are being asked to do online (including what sites they will be asked to access) and who from the School they will be interacting with online, if anyone.

12.3.2 The School works closely with parents to ensure they can safeguard their children whilst using technology. Information is regularly sent through the newsletter and via talks for parents. Parents are also advised upon best practice and introduced to current trends during tutorial evenings.

12.3.3 Parents are encouraged to read the Acceptable Use of ICT Policy for Pupils with their child to ensure that it is fully understood.

12.3.4 Parents have an important role in supporting the School's policy on prohibiting the use of mobile phones. Parents are encouraged to reinforce and discuss this policy with pupils, including the risks associated with mobile phone use and the benefits of a mobile phone free environment.

12.3.5 Where parents need to contact their child during the school day, they should be directed to the school office, where staff should be aware of the school's policy on relaying messages and facilitating contact.

12.3.6 **Useful online safety resources for parents**

(a) https://www.saferinternet.org.uk/advice-centre/parents-and-carers

(b) http://www.childnet.com/parents-and-carers

(c) https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online-safety/

(d) https://www.thinkuknow.co.uk/parents/

(e) https://www.thinkuknow.co.uk/parents/articles/theres-a-viral-scare-online-what-should-i-do/

(f) http://parentzone.org.uk/

(g) https://www.internetmatters.org/

(h) https://www.commonsensemedia.org/

(i) Advice for parents and carers on cyberbullying (DfE, November 2014)

(j) https://www.askaboutgames.com/

(k) https://www.ceop.police.uk/safety-centre

(l) UK Chief Medical Officers' advice for parents and carers on children and young people's screen and social media use (February 2019)

(m) https://safeblog.lgfl.net/2018/11/parents-scare-or-prepare

(n) Thinkuknow: what to do if there's a viral scare online

(o) AI Child Sexual Abuse Imagery: Parent Safety Guide

13 Cybercrime

13.1 Cybercrime is criminal activity committed using computers and/or the internet. It is broadly categorised as either 'cyber-enabled' (crimes that can happen off-line but are enabled at scale

and at speed on-line) or 'cyber dependent' (crimes that can be committed only by using a computer).

13.2 Cyber-dependent crimes include;

13.2.1 unauthorised access to computers (illegal 'hacking'), for example, accessing a school's computer network to look for test paper answers or change grades awarded;

13.2.2 denial of service (DoS or DDoS) attacks or 'booting', which are attempts to make a computer, network or website unavailable by overwhelming it with internet traffic from multiple sources; and

13.2.3 making, supplying or obtaining malware (malicious software) such as viruses, spyware, ransomware, botnets and Remote Access Trojans with the intent to commit further offence, including those above.

13.3 The School is aware that pupils with particular skill and interest in computing and technology may inadvertently or deliberately stray into cyber-dependent crime.

13.4 The School will take appropriate action to meet the Cyber security standards to improve resilience against cyber-attacks.

13.5 If staff have any concerns about a child in this area, they should refer the matter to the Designated Safeguarding Lead immediately. The Designated safeguarding Lead should then consider referring into the Cyber Choices programme. This is a nationwide police programme supported by the Home Office and led by the National Crime Agency, working with regional and local policing. It aims to intervene where young people are at risk of committing, or being drawn into, low level cyber-dependent offences and divert them to a more positive use of their skills and interests. Cyber Choices does not currently cover 'cyber-enabled' crime such as fraud, purchasing of illegal drugs on-line and child sexual abuse and exploitation, nor other areas of concern such as on-line bullying or general on-line safety.

14 Risk assessment

14.1 The School recognises that technology, and the risks and harms associated with it, evolve and change rapidly. The School will carry out regular, and at least annual, reviews of its approach to online safety, supported by risk assessments which consider and reflect the risks faced by its pupils.

14.2 Where a concern about a pupil's welfare is identified, the risks to that pupil's welfare will be assessed and appropriate action will be taken to reduce the risks identified.

14.3 The format of risk assessment may vary and may be included as part of the School's overall response to a welfare issue, including the use of individual pupil welfare plans (such as behaviour, healthcare and education plans, as appropriate). Regardless of the form used, the School's approach to promoting pupil welfare will be systematic and pupil focused.

14.4 The Head has overall responsibility for ensuring that matters which affect pupil welfare are adequately risk assessed and for ensuring that the relevant findings are implemented, monitored and evaluated.

14.5 Day to day responsibility to carry out risk assessments under this policy will be delegated to Deputy Head (Pupil development and welfare), Prep Deputy Head or Pelican Deputy Head (as appropriate) who have been properly trained in, and tasked with, carrying out the particular assessment.

15 Record keeping

15.1 All records created in accordance with this policy are managed in accordance with the School's policies that apply to the retention and destruction of records.

15.2 All serious incidents involving the use of technology will be logged centrally in the IT incident log by the Director of ICT and as part of the pupil or staff record.

15.3 The information created in connection with this policy may contain personal data. The School's use of personal data will be in accordance with data protection law. The School has published privacy notices on its website which explain how the School will use personal data. The School's approach to data protection compliance is set out in the School's data protection policies and procedures when handling personal data created in connection with this policy. In addition, staff must ensure that they follow the School's data protection policies and procedures. This includes the School's Data Protection Policy and Information Security and Sharing Data Guidance.

16 Version control

Date of adoption of this policy	3 September 2026
Date of last review of this policy	August 2026
Date for next review of this policy	August 2027
Policy owner (SMT)	Designated Safeguarding Lead (Upper, Prep and Pelican)
Authorised by	Jonathan Scott On behalf of the Board of Governors
Circulation	Governors / teaching staff / all staff / all parents / Upper pupils Published on the School's website and Perse Portal and available from the School Office on request