



**THE PERSE**  
**SCHOOL**  
CAMBRIDGE

## **Online Safety Policy**

---

**The Perse School**

September 2021

## 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 .....	3
7	Role of staff and parents.....	4
8	Access to the School's technology.....	7
9	Procedures for dealing with incidents of misuse.....	9
10	Education .....	10
11	Training .....	12
12	Cybercrime .....	14
13	Risk assessment .....	15
14	Record keeping .....	15
15	Version control.....	17

## 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:
  - 1.2.1 protects the whole School community from illegal, inappropriate and harmful content or contact;
  - 1.2.2 educates the whole School community about their access to and use of technology;
  - 1.2.3 establishes effective mechanisms to identify, intervene and escalate incidents where appropriate; and
  - 1.2.4 promotes a whole school culture of safety, equality and protection.
- 1.3 This policy forms part of the School's whole school approach to promoting child safeguarding and wellbeing, which seeks to ensure that the best interests of pupils underpins and is at the heart of all decisions, systems, processes and policies.
- 1.4 Online safety is a running and interrelated theme throughout 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.

## 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 Statutory framework for the Early Years Foundation Stage (DfE, September 2021);
  - 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
  - 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 \(DfE, September 2021\)](#);
  - 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 \(December 2020\)](#);
  - 3.2.4 [Revised Prevent duty guidance: for England and Wales \(Home Office, April 2021\)](#);
  - 3.2.5 [Channel duty guidance: protecting vulnerable people from being drawn into terrorism \(Home Office, February 2021\)](#).
  - 3.2.6 [Sexual violence and sexual harassment between children in schools and colleges \(DfE, September 2021\)](#);
  - 3.2.7 [Relationships Education, Relationships and Sex Education \(RSE\) and Health Education guidance \(DfE, February 2019\)](#);
  - 3.2.8 [Searching, screening and confiscation: advice for schools \(DfE, January 2018\)](#);
  - 3.2.1 [Teaching online safety in schools \(DfE, June 2019\)](#);
  - 3.2.2 [Harmful online challenges and online hoaxes \(DfE, February 2021\)](#);
  - 3.2.3 [Online safety guidance if you own or manage an online platform \(DfDCMS, June 2021\)](#);
  - 3.2.4 [A business guide for protecting children on your online platform \(DfDCMS, June 2021\)](#); and
  - 3.2.5 [Online safety audit tool \(UKCIS, August 2020\)](#).
- 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 Risk Assessment Policy for Pupil Welfare;
  - 3.3.6 Staff Code of Conduct and Whistleblowing Policy;
  - 3.3.7 Data Protection Policy for Staff;
  - 3.3.8 Relationships Education and Relationships and Sex Education policy; and
  - 3.3.9 Information Security and Sharing Data Guidance.

#### 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** are references to the Designated Safeguarding Lead for the Relevant School
  - 5.1.2 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.
- 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:

<b>Task</b>	<b>Allocated to</b>	<b>When / frequency of review</b>
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 termly
Monitoring the implementation of the policy, including the record of 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	Upper School - Deputy Head (Pupil development and welfare) Prep School – Deputy Head Pelican School – Deputy Head	As required, and at least termly

Online safety	Designated Safeguarding Leads	As required, and at least termly
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
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.
- 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. The responsibility of the Designated Safeguarding Lead includes managing safeguarding incidents involving the use of technology in the same way as other safeguarding matters, in accordance with the School's safeguarding and child protection policy.
- 7.1.3 The Designated Safeguarding Lead will work with the Director of ICT (see below) in monitoring technology uses and practices across the School and assessing whether any improvements can be made to ensure the online safety and well-being of pupils.
- 7.1.4 The Designated Safeguarding Lead will periodically collect information from staff, pupils and parents to inform updates to the policy and online safety procedures.
- 7.1.5 The Designated Safeguarding Lead will regularly monitor the technology incident log maintained by the Director of ICT.
- 7.1.6 The Designated Safeguarding Lead will regularly update other members of the School's Senior Leadership Team on the operation of the School's safeguarding arrangements, including online safety practices.

### 7.2 Director of ICT

- 7.2.1 The Director of ICT together with their team, is responsible for the effective operation of the School's filtering system 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.
- 7.2.2 The Director of ICT is responsible for ensuring that:
- (a) the School's technology infrastructure is secure and, so far as is possible, is not open to misuse or malicious attack;
  - (b) the user may only use the School's technology if they are properly authenticated and authorised;

- (c) the School has an effective filtering policy in place and that it is applied and updated on a regular basis;
- (d) the risks of pupils and staff circumventing the safeguards put in place by the School are minimised;
- (e) 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
- (f) 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.

7.2.3 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 monitors the type of emails (SPAM, Virus etc..) and reports verbally to the Senior Bursary Team and Senior Leadership Team on a weekly basis.
- (c) The Director of ICT receives a daily email from the 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.
- (d) Email alerts are setup on the school file server alerting senior IT staff if a disallowed file type has been saved on the computer network. E.g virus or .exe file

7.2.4 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, suitability or use of technology within the School, including of the monitoring and filtering systems in place, they will escalate those concerns promptly to the Designated Safeguarding Lead.

7.2.5 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*.

### 7.3 All staff

7.3.1 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.

7.3.2 All staff are aware that technology 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.

- 7.3.3 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 sharing of indecent images and videos (especially around group chats), which is sometimes known as sexting or youth produced sexual imagery;
  - (c) the sharing of abusive images and pornography to those who do not wish to receive such content; and/or
  - (d) cyberbullying,
- 7.3.4 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.
- 7.3.5 It is important that staff recognise the indicators and signs of peer on peer 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 peer on peer 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.
- 7.3.6 It is important that staff challenge inappropriate behaviours between peers and do not downplay certain behaviours, including 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 behaviours, an unsafe environment for children and, in a worst case scenario, a culture that normalises abuse. The School has a **zero tolerance approach** towards peer on peer abuse (including in relation to 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.
- 7.3.7 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 peer on peer 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**.

## 7.4 Parents

7.4.1 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; and
- (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.

7.4.2 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 11.2.3.

## 8 Access to the School's technology

8.1 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.

8.2 Pupils and staff require individual user names 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 user names or passwords must report it to the IT department immediately.

8.3 The use of any personal device connected to the School's WI-FI network will be logged and monitored by the IT department. See also 8.5 below.

8.4 The School has a separate Wi-Fi connection available for use by visitors to the School. A password, which is changed on a regular basis, must be obtained from a member of staff in order to use the Wi-Fi. Use of this service will be logged and monitored by the IT department.

### 8.5 Inappropriate material

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

8.5.2 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 issues but these can be classified into four main areas of risk:

- (a) **Content** - being exposed to illegal, inappropriate or harmful content (e.g. pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism);

- (b) **Contact** - being subjected to harmful online interaction with other users (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 consensual and non-consensual 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.

## 8.6 Use of mobile electronic devices and smart technology

- 8.6.1 The School has appropriate filtering and monitoring systems in place to protect pupils using the internet (including email and social media sites) when connected to the School's network.
- 8.6.2 Mobile devices and smart technology equipped with a mobile data subscription can provide unlimited and unrestricted access to the internet. Since the School cannot put adequate protection for pupils in place,
  - (a) Pelican School pupils are not permitted to have mobile phones in School under any circumstances;
  - (b) Prep School pupils must leave phones and other mobile devices with reception during the school day; and
  - (c) Upper School pupils are not allowed to use their mobile devices when in the School's care except in the PAC Café, and the Library whilst supervised or with specific permission from a member of staff for a specified task. Sixth form pupils may also use mobile devices in the Sixth Form areas.
- 8.6.3 The School is alert to the risks that such access presents, including the risk of pupils sexually harassing their peers using their mobile or other smart technology; or sharing indecent images consensually or non-consensually; or viewing and/or sharing pornography and other harmful content, and has mechanisms in place to manage such risks.
- 8.6.4 The School rules about the use of mobile electronic devices or other smart technology, including access to open/non-School networks, are set out in the acceptable use of ICT policy for pupils.
- 8.6.5 The use of mobile electronic devices by staff is covered in the staff code of conduct.
- 8.6.6 The School's policies apply to the use of technology by staff and pupils whether on or off School premises and appropriate action will be taken where such use 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.
- 8.6.7 School devices used by pupils in Year 9-11 are monitored continuously, even outside of the School site. Pupils may only use them for educational purposes.

## 9 Procedures for dealing with incidents of misuse

9.1 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.

9.2 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.

### 9.3 Misuse by pupils

9.3.1 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.
Other breach of acceptable use policy	See relevant policy referred to in acceptable use policy	Note any incidents which give rise to safeguarding concerns must be referred on to the Designated Safeguarding Lead
Sharing nudes and semi-nude images (sexting / youth produced sexual imagery)	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
Sexual violence and sexual harassment (whether during or outside of school)	Safeguarding and child protection policy	
Harassment	Safeguarding and child protection policy	
Upskirting	Safeguarding and child protection policy	

Radicalisation	Safeguarding and child protection policy	
----------------	--	--

9.3.2 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*).

#### 9.4 **Misuse by staff**

9.4.1 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.

9.4.2 If anyone has a safeguarding-related concern relating to staff misuse of technology, they should be report it immediately so that it can be dealt with in accordance with the procedures for reporting and dealing with allegations of abuse against staff set out in the School's *Safeguarding and Child Protection Policy*.

#### 9.5 **Misuse by any user**

9.5.1 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.

9.5.2 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.

9.5.3 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.

### 10 **Education**

10.1 The safe use of technology is 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.

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

10.2.1 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;

10.2.2 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

- 10.2.3 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.
- 10.3 The safe use of technology is also a focus in all areas of the curriculum teacher training and key safety messages are reinforced as part of assemblies, PSHE and tutorial / pastoral activities, teaching pupils:
- 10.3.1 about the risks associated with using the technology and how to protect themselves and their peers from potential risks;
  - 10.3.2 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";
  - 10.3.3 to be critically aware of content they access online and guided to validate accuracy of information;
  - 10.3.4 how to recognise suspicious, bullying or extremist behaviour;
  - 10.3.5 the definition of cyberbullying, its effects on the victim and how to treat each other's online identities with respect;
  - 10.3.6 relevant laws applicable to the internet
  - 10.3.7 the consequences of negative online behaviour;
  - 10.3.8 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
  - 10.3.9 how to respond to harmful online challenges and hoaxes.
- 10.4 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 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.
- 10.5 The safe use of technology aspects of the curriculum are reviewed on a regular basis to ensure their relevance.
- 10.6 The School's *Acceptable Use of ICT Policy for Pupils* sets out the School rules about the use of 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.
- 10.7 **Useful online safety resources for pupils**
- 10.7.1 <http://www.thinkuknow.co.uk/>
  - 10.7.2 <http://www.childnet.com/young-people>
  - 10.7.3 <https://www.saferinternet.org.uk/advice-centre/young-people>

- 10.7.4 <https://www.disrespectnobody.co.uk/>
- 10.7.5 <https://mysafetynet.org.uk/>
- 10.7.6 <https://www.ceop.police.uk/Safety-Centre/How-can-CEOP-help-me-YP/>
- 10.7.7 <https://www.bbc.com/ownit>
- 10.7.8 <https://www.gov.uk/government/publications/indecent-images-of-children-guidance-for-young-people/indecent-images-of-children-guidance-for-young-people>

## 11 Training

### 11.1 Staff

- 11.1.1 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.
- 11.1.2 Induction training for new staff includes training on the School's online safety strategy including this policy, the *Code of Conduct* and *Acceptable Use of ICT Policy for Staff*. Ongoing staff development training includes training on technology safety together with specific safeguarding issues including sharing nudes and semi-nudes images and or videos,, cyberbullying and radicalisation and dealing with harmful online challenges and hoaxes.
- 11.1.3 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 sexual violence or sexual harassment, and nor should they ever be made to feel ashamed for making a report.
- 11.1.4 Where safeguarding incidents involve an online element, such as youth produced sexual imagery, staff will not view or forward sexual imagery reported to them and will follow the School's policy on sharing nudes and semi-nude images and videos as set out in Appendix 1 of the School's Safeguarding and Child Protection Policy and Procedures and *Searching, screening and confiscation: advice for schools* (DfE, January 2018). 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.
- 11.1.5 Staff are encouraged to adopt and maintain an attitude of 'it could happen here' in relation to 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
- 11.1.6 Staff are trained 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.

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

11.1.8 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.

**11.1.9 Useful online safety resources for staff**

- (a) <https://www.lgfl.net/online-safety/default.aspx>
- (b) <https://www.saferinternet.org.uk/advice-centre/teachers-and-professionals>
- (c) <http://www.childnet.com/teachers-and-professionals>
- (d) <https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online-safety/>
- (e) <https://www.thinkuknow.co.uk/teachers/>
- (f) <http://educateagainsthate.com/>
- (g) <https://www.commonsense.org/education/>
- (h) Cyberbullying: advice for head teachers and school staff (DfE, November 2014)
- (i) Advice on the use of social media for online radicalisation (DfE and Home Office, July 2015)
- (j) Sharing nudes and semi-nudes: advice for education settings working with children and young people (December 2020).
- (k) Online safety in schools and colleges: questions from the governing board (UKCCIS, 2020)
- (l) Education for a connected world framework (UKCCIS, 2020)
- (m) Online Sexual Harassment: Understand, Prevent and Respond Guidance for Schools (Childnet, March 2019)
- (n) Myth vs Reality: PSHE toolkit (Childnet, April 2019)
- (o) SELMA Hack online hate toolkit (SWGFL, May 2019)
- (p) Teaching online safety in school: Guidance supporting schools to teach their pupils how to stay safe online, within new and existing school subjects (June 2019)
- (q) Harmful online challenges and online hoaxes (DfE, February 2021)
- (r) Professionals online safety helpline: [helpline@saferinternet.org.uk](mailto:helpline@saferinternet.org.uk), 0344 381 4772
- (s) NSPCC helpline for anyone worried about a child - 0808 800 5000

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

11.1.1 The Cambridgeshire and Peterborough Safeguarding Partnership has produced guidance on radicalisation which is available here: <https://safeguardingcambspeterborough.org.uk/children-board/professionals/prevent/>.

## 11.2 Parents

11.2.1 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.

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

### 11.2.3 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) <http://parentinfo.org/>
- (f) <http://parentzone.org.uk/>
- (g) <https://www.net-aware.org.uk>
- (h) <https://www.internetmatters.org/>
- (i) <https://www.common sense media.org/>
- (j) Advice for parents and carers on cyberbullying (DfE, November 2014)
- (k) <https://www.askaboutgames.com/>
- (l) <https://www.ceop.police.uk/safety-centre>
- (m) UK Chief Medical Officers' advice for parents and carers on children and young people's screen and social media use (February 2019)

## 12 Cybercrime

12.1 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).

12.2 Cyber-dependent crimes include;

- 12.2.1 unauthorised access to computers (illegal 'hacking'), for example, accessing a school's computer network to look for test paper answers or change grades awarded;
  - 12.2.2 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
  - 12.2.3 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.
- 12.3 The School is aware that pupils with particular skill and interest in computing and technology may inadvertently or deliberately stray into cyber-dependent crime.
- 12.4 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.

### **13 Risk assessment**

- 13.1 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.
- 13.2 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.
- 13.3 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.
- 13.4 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.

### **14 Record keeping**

- 14.1 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.
- 14.2 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.
- 14.3 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. This includes the School's *Data Protection Policy* and *Information Security and Sharing Data Guidance*, which are contained in the *Data Protection and Information Security Handbook*.

15 **Version control**

Date of adoption of this policy	6 <sup>th</sup> September 2021
Date of last review of this policy	August 2021
Date for next review of this policy	August 2022
Policy owner (SMT)	Deputy Head (Pupil development and welfare) – Upper School Deputy Head - Prep School Deputy Head – Pelican School
Authorised by	<hr/> 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