THE PERSE SCHOOL
CAMBRIDGE

Online Safety Policy

The Perse School

September 2018

VWV

Contents

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; and

1.2.3 establishes effective mechanisms to identify, intervene and escalate incidents where appropriate.

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.

2.3 This policy relates to current and emerging technologies and includes, but is not limited to, websites, email, instant messaging, blogging, social networking sites, chat rooms, media downloads, gaming sites, text and picture messaging, video calls, podcasting, online communities, mobile devices, cloud technologies and online learning platforms.

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, March 2017);

3.1.3 Education and Skills Act 2008;

3.1.4 Childcare Act 2006;

3.1.5 Data Protection Act 2018 and General Data Protection Regulation (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 2018);

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

3.2.3 Sexting in schools and colleges: responding to incidents and safeguarding young people (UK Council for Child Internet Safety, August 2016);

3.2.4 Prevent duty guidance for England and Wales (Home Office, July 2015);

3.2.5 Channel duty guidance: protecting vulnerable people from being drawn into terrorism (Home Office, April 2015).

3.2.6 Sexual violence and sexual harassment between children in schools and colleges (DfE, December 2017); and

3.2.7 Searching, screening and confiscation: advice for schools (DfE, January 2018).

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 IT policy for staff and staff guidance on using social media;

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 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:

References to **Designated Safeguarding Lead** are references to the Designated Safeguarding Lead for the Relevant School

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**). See 2.3 above for examples of the types of technologies covered by this policy.

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:

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 (Pupils) 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	Upper School - Deputy Head (Pupils) Prep School – Deputy Head Pelican School – Deputy Head	As required, and at least termly
Maintaining up to date records of all information created in relation to the policy and its implementation as required by the GDPR	Director of ICT	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 (Pupils) 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 Management 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 5 of the acceptable use of IT policy for staff outlines the School's Technical Infrastructure and Reporting Mechanisms. In summary:

- 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 issues and potential problems on the network.
- The Director of ICT monitors the type of emails (SPAM, Virus etc..) and reports verbally to the Senior Bursary Team and Senior Management Team termly, but more often if needed.
- 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.

• 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 Management 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 Staff are expected to adhere, so far as applicable, to each of the policies referenced in this policy.

7.3.3 Staff are responsible for promoting and supporting safe behaviours in their classrooms. When pupils use school IT or technology whilst in the care of school, staff should ensure that supervision is appropriate for the pupils involved.

7.3.4 Staff should raise concerns about online safety with the Director of ICT or Designated Safeguarding Lead.

7.3.5 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.

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 IT 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 WIFI 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 **Use of mobile electronic devices**

8.5.1 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.

8.5.2 Mobile devices 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 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.

8.5.3 The School rules about the use of mobile electronic devices are set out in the acceptable use of ICT policy for pupils.

8.5.4 The use of mobile electronic devices by staff is covered in the code of conduct.

8.5.5 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.

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 **Misuse by pupils**

9.2.1 Anyone who has any concern about the misuse of technology by pupils should report it 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.

9.2.2 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).

9.3 **Misuse by staff**

9.3.1 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.

9.3.2 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.

9.4 **Misuse by any user**

9.4.1 Anyone who has a 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.

9.4.2 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.

9.4.3 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 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 to be critically aware of content they access online and guided to validate accuracy of information;

10.3.3 how to recognise suspicious, bullying or extremist behaviour;

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

10.3.5 relevant laws applicable to the internet

10.3.6 the consequences of negative online behaviour; and

10.3.7 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.

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

10.5 The School's acceptable use policy of ICT 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.

10.6 **Useful online safety resources for pupils**

10.6.1 http://www.thinkuknow.co.uk/

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

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

10.6.4 https://www.disrespectnobody.co.uk/

10.6.5 http://www.safetynetkids.org.uk/

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 IT policy for

staff. Ongoing staff development training includes training on technology safety together with specific safeguarding issues including sexting, cyberbullying and radicalisation.

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

11.1.4 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.

11.1.5 **Useful online safety resources for staff**

(a) http://swgfl.org.uk/products-services/esafety

(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) Sexting in schools and colleges: responding to incidents and safeguarding young people (UK Council for Child Internet Safety (UKCCIS), August 2016).

(k) Online safety in schools and colleges: questions from the governing board (UKCCIS, 2016)

(l) Education for a connected world framework (UKCCIS)

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

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 son / daughter 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.commonsensemedia.org/

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

12 Record keeping

12.1 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.

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

12.3 The records created in accordance with this policy may contain personal data. The School has a number of privacy notices which explain how the School will use personal data about pupils and parents. The privacy notices are published on the School's website. In addition, staff must ensure that they follow 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.

13 Version control

Date of adoption of this policy	03 September 2018
Date of last review of this policy	03 September 2018
Date for next review of this policy	June 2019
Policy owner (SMT)	Deputy Head (Pupils) – Upper School Deputy Head - Prep School Deputy Head – Pelican School
Authorised by	Sir David Wright 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