QUI FACIT PER ALIUM FACIT PER SE

THE PERSE
SCHOOL
CAMBRIDGE

Acceptable Use of ICT Policy for Pupils

The Perse School

September 2018

vwv

Contents

Clause

Appendix

1 Aims

1.1 This is the acceptable use of ICT policy for pupils 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 aims of this policy are as follows:

1.2.1 to educate and encourage pupils to make good use of the educational opportunities presented by access to technology;

1.2.2 to safeguard and promote the welfare of pupils, in particular by anticipating and preventing the risks arising from:

(a) exposure to harmful or inappropriate material (such as pornographic, racist, extremist or offensive materials);

(b) the sharing of personal data, including images;

(c) inappropriate online contact or conduct; and

(d) cyberbullying and other forms of abuse.

1.2.3 to minimise the risk of harm to the assets and reputation of the School;

1.2.4 to help pupils take responsibility for their own safe use of technology;

1.2.5 to ensure that pupils use technology safely and securely and are aware of both external and peer-to-peer risks when using technology; and

1.2.6 to prevent the unnecessary criminalisation of pupils.

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 the use of technology at all times when a pupil is:

2.2.1 in or at school;

2.2.2 representing the School or wearing School uniform;

2.2.3 travelling to or from School;

2.2.4 on School-organised trips; or

2.2.5 associated with the School at any time.

2.3 This policy shall also apply to pupils at all times and places in circumstances where failing to apply this policy may:

2.3.1 affect the health, safety or well-being of a member of the School community or a member of the public;

2.3.2 have repercussions for the orderly running of the School; or

2.3.3 bring the School into disrepute.

2.4 Parents are encouraged to read this policy with their child. The School actively promotes the participation of parents to help the School safeguard the welfare of pupils and promote the safe use of technology.

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 Sexual violence and sexual harassment between children in schools and colleges (DfE, May 2018); and

3.2.5 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 Behaviour And Discipline Policy;

3.3.2 Anti-Bullying Policy (Pupils);

3.3.3 Online Safety Policy;

3.3.4 Permanent Exclusion And Removal: Review Procedure;

3.3.5 Safeguarding Policy And Child Protection Policy Procedures; and

3.3.6 Risk Assessment Policy For Pupil Welfare.

4 Publication and availability

4.1 This policy is available in hard copy on request.

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

4.3 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 the **Head** are references to the Head of the Relevant School.

5.2 The School will take a wide and purposive approach to considering what falls within the meaning of **technology**. This policy relates to all technology, computing and communications devices, network hardware and software and services and applications associated with them including:

5.2.1 the internet;

5.2.2 email;

5.2.3 mobile phones and smartphones;

5.2.4 desktops, laptops, netbooks, tablets / phablets;

5.2.5 personal music players;

5.2.6 devices with the capability for recording and / or storing still or moving images;

5.2.7 social networking, micro blogging and other interactive websites;

5.2.8 instant messaging (including image and video messaging via apps such as Snapchat and WhatsApp), chat rooms, blogs and message boards;

5.2.9 webcams, video hosting sites (such as YouTube);

5.2.10 gaming sites;

5.2.11 virtual learning environments such as Schoology];

5.2.12 SMART boards; and

5.2.13 other photographic or electronic equipment e.g. GoPro devices.

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 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	Deputy Head (Pupils) and the Director of ICT	As required, and at least termly
Monitoring the use of technology across the School, maintaining appropriate logs and reviewing the policy to ensure that it remains up to date with technological change	Director of ICT	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	Deputy Head (Pupils) and the Director of ICT	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	Director of ICT	As required, and at least annually
Formal annual review	Board of Governors	Annually

7 Safe use of technology

7.1 We want pupils to enjoy using technology and to become skilled users of online resources and media. We recognise that this is crucial for further education and careers.

7.2 The School will support pupils to develop their skills and make internet access as unrestricted as possible whilst balancing the safety and welfare of pupils and the security of our systems. The safe use of technology is integral to the School's curriculum. Pupils are educated about the importance of safe and responsible use of technology to help them to protect themselves and others online.

7.3 Pupils may find the following resources helpful in keeping themselves safe online:

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

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

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

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

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

7.3.6 http://www.childline.org.uk/Pages/Home.aspx

7.4 Please see the School's online safety policy for further information about the School's online safety strategy.

8 Internet and email

8.1 The School provides internet access and, in Year 5 and above, an email system to pupils to support their academic progress and development.

8.2 All pupils will receive guidance on the use of the School's internet and, where accessible, email systems. If a pupil is unsure about whether they are doing the right thing, they must seek assistance from a member of staff.

8.3 For the protection of all pupils, their use of email and of the internet will be monitored by the School. Pupils should remember that even when an email or something that has been downloaded has been deleted, it can still be traced on the system. Pupils should not assume that files stored on servers or storage media are always private.

9 School rules

9.1 Pupils **must** comply with the following rules and principles:

9.1.1 access and security (Appendix 1);

9.1.2 use of internet and email (Appendix 2);

9.1.3 use of mobile electronic devices (Appendix 3); and

9.1.4 photographs and images (including "sexting") (Appendix 4).

These rules are condensed into a ‘pupil-friendly’ poster displayed in appropriate locations at each school (Appendix 5).

9.2 The purpose of these rules is to set out the principles which pupils must bear in mind at all times and also the rules which pupils must follow to use technology safely and securely.

9.3 These principles and rules apply to all use of technology.

10 Procedures

10.1 Pupils are responsible for their actions, conduct and behaviour when using technology at all times. Use of technology should be safe, responsible and respectful to others and the law. If a pupil is aware of misuse by other pupils they should talk to a teacher about it as soon as possible.

10.2 Any misuse of technology by pupils will be dealt with under the School's behaviour and discipline policy.

10.3 Pupils must not use their own or the School's technology to bully others. Bullying incidents involving the use of technology will be dealt with under the School's anti-bullying policy (pupils). If a pupil thinks that they might have been bullied or that another person is being bullied, they should talk to a teacher about it as soon as possible. See the School's anti-bullying policy (Pupils) for further information about cyberbullying and e-safety, including useful resources.

10.4 The Designated Safeguarding Lead takes lead responsibility within the School for safeguarding and child protection, including online safety. In any cases giving rise to safeguarding concerns, the matter will be dealt with under the School's child protection procedures (see the School's safeguarding and child protection policy). If a pupil is worried about something that they have seen on the internet, or on any electronic device, including on another person's electronic device, they must tell a teacher about it as soon as possible.

10.5 In a case where the pupil is considered to be vulnerable to radicalisation they may be referred to the Channel programme. Channel is a programme which focuses on support at an early stage to people who are identified as being vulnerable to being drawn into extremism (including terrorism).

10.6 In addition to following the procedures in the relevant policies as set out above, all serious incidents involving technology must be reported to the Deputy Head (Pupils) or the Director of ICT who will record the matter centrally in the technology incidents log.

11 Sanctions

11.1 Where a pupil breaches any of the School rules, practices or procedures set out in this policy or the appendices, the Board of Governors has authorised the Head to apply any sanction which is appropriate and proportionate to the breach in accordance with the School's behaviour and discipline policy including, in the most serious cases, permanent exclusion.

11.2 Unacceptable use of technology could lead to the confiscation of a device or deletion of the material in accordance with the procedures in this policy and sections 6, 7.10 and 7.11 of the School's policy on searching and the retention and disposal of confiscated items.

11.3 If there are reasonable grounds to suspect that the confiscated device contains evidence in relation to an offence, or that it contains a pornographic image of a child or an extreme pornographic image, the device will be given to the police. See Appendix 4 for more information on photographs and images.

11.4 The School reserves the right to charge a pupil or their parents for any costs incurred to the School as a result of a breach of this policy.

12 Training

12.1 The School ensures that regular guidance and training is arranged on induction and at regular intervals thereafter so that staff and volunteers understand what is expected of them by this policy and have the necessary knowledge and skills to carry out their roles.

12.2 The level and frequency of training depends on role of the individual member of staff.

13 Record keeping

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

13.2 All serious incidents involving the use of technology will be logged centrally in the technology incident log by the Director of ICT.

13.3 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.

14 Version control

Date of adoption of this policy	3 September 2018
Date of last review of this policy	November 2015
Date for next review of this policy	March 2019
Policy owner (SMT)	Director of ICT
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

Appendix 1 Access and security

1 Access to the internet from the School's computers and network must be for educational purposes only.

2 You must not knowingly obtain (or attempt to obtain) unauthorised access to any part of the School's or any other computer system, or any information contained on such a system.

3 Use of any pupil laptop or other mobile device connected to the School's wifi is also covered by this policy regarding acceptable behaviour.

4 The use of cellular data (e.g. GPRS, 3G, 4G, etc) to access the internet while pupils are on School premises or otherwise in the care of the School should only be done in the designated locations, as pupils are unable to benefit from the School's filtering and anti-virus software. Pupils accessing the internet outside the School's network whilst on School premises or otherwise in the care of the School do so at their own risk and must comply with all the provisions of this policy regarding acceptable behaviour. If a pupil's device can access the internet outside of the school wifi network then parents must ensure their child's device has appropriate security enabled.

5 Passwords protect the School's network and computer system. You must not let anyone else know your password. If you believe that someone knows your password you must change it immediately.

6 You must not attempt to gain unauthorised access to anyone else's computer or to confidential information to which you are not authorised to access. If there is a problem with your passwords, you should speak to your class teacher or contact the Director of ICT

7 You must not attempt to access or share information about others without the permission of the Director of ICT. To do so may breach data protection legislation and laws relating to confidentiality.

8 The School has a firewall in place to ensure the safety and security of the School's networks. You must not attempt to disable, defeat or circumvent any of the School's security facilities. Any problems with the firewall must be reported to the class teacher or the Director of IT

9 The School has filtering systems in place to block access to unsuitable material, wherever possible, to protect the welfare and safety of pupils. You must not try to bypass this filter.

10 Viruses can cause serious harm to the security of the School's network and that of others. Viruses are often spread through internet downloads or circulated as attachments to emails. If you think or suspect that an attachment, or other downloadable material, might contain a virus, you must speak to a member of the IT team before opening the attachment or downloading the material.

11 You must not disable or uninstall any anti-virus software on the School's computers.

12 The use of location services represents a risk to the personal safety of pupils and to School security. The use of any website or application, whether on a School or personal device, with the capability of identifying the user's location while you are on School premises or otherwise in the care of the School is discouraged.

Appendix 2 Use of the internet and email

1 The School does not undertake to provide continuous internet access. Email and website addresses at the School may change from time to time.

Use of the internet

2 You must take care to protect personal and confidential information about yourself and others when using the internet, even if information is obtained inadvertently. You should not put personal information about yourself, for example your full name, address, date of birth or mobile number, online.

3 You should assume that all material on the internet is protected by copyright and such material must be treated appropriately and in accordance with the owner's rights - you must not copy (plagiarise) another's work.

4 You must not view, retrieve, download or share any offensive material. Offensive material includes, but is not limited to, content that is abusive, racist, considered to be of an extreme or terrorist related nature, sexist, homophobic, any form of bullying, pornographic, defamatory or criminal activity. Use of technology in this way is a serious breach of discipline and may constitute a serious criminal offence. You must tell a member of staff immediately if you have accidentally read, downloaded or have been sent any offensive material or material that is inappropriate, including personal information about someone else.

5 You must not communicate with staff using social networking sites or other internet or web-based communication channels.

6 You must not bring the School into disrepute through your use of the internet.

Use of email

7 Your School email accounts can be accessed from home by going to https://mail.perse.co.uk/owa

8 You must use your School email accounts for any email communication with staff. Communication either from a personal email account or to a member of staff's personal email account is not permitted.

9 Email should be treated in the same way as any other form of written communication. You should not include or ask to receive anything in an email which is not appropriate to be published generally or which you believe the School and / or your parents would consider to be inappropriate. Remember that emails could be forwarded to or seen by someone you did not intend.

10 You must not send or search for any email message which contains offensive material. Offensive material includes, but is not limited to, content that is abusive, racist, considered to be of an extreme or terrorist related nature, sexist, homophobic, any form of bullying, pornographic, defamatory or criminal activity. If you are unsure about the content of a message, you must speak to a member of staff. If you come across such material you must inform a member of staff as soon as possible. Use of the email system in this way is a serious breach of discipline and may constitute a criminal offence.

11 Trivial messages and jokes should not be sent or forwarded through the School's email system. Not only could these cause distress to recipients (if considered to be inappropriate) but could also cause the School's network to suffer delays and / or damage.

12 All correspondence from your School email account must contain the School's disclaimer.

13 You must not read anyone else's emails without their consent.

Appendix 3 Use of mobile electronic devices

1 **Mobile electronic device** includes but is not limited to mobile phones, smartphones, tablets, laptops and MP3 players.

2 In the Upper School Mobile phones and other mobile electronic devices must be switched off (and not just on silent mode) and kept out of sight during School hours, including at break times and between lessons. The exception is that the use of such devices at the Upper is only permitted in designated locations (Café, Library and Sixth form area) or with express permission from a member of staff for a specific purpose and time.

3 Pupils in the Pelican School are not permitted to have mobile phones in school under any circumstances.

4 Pupils in the Prep School may not bring mobile phones to school unless required for travelling to school via public transport. Those pupils must leave their phone at reception before school and collect it at the end of the day. The School has a list of those pupils permitted to bring in a mobile phone and all devices are stored in a secure, lockable case during the day.

5 In emergencies, you may request to use the School telephone. Should your parents wish to contact you in an emergency, they will telephone the School and a message will be relayed promptly.

6 You must not bring mobile electronic devices into examination rooms under any circumstances, except where special arrangements for the use of a tablet or laptop have been agreed by the Exams Officer.

7 Pupils may use specified devices as part of a learning support plan only for the purposes stated in the plan.

8 You must not communicate with staff using a mobile phone (or other mobile electronic device) except when this is expressly permitted by a member of staff, for example when necessary during an educational visit. Any such permitted communications should be brief and courteous.

9 Use of electronic devices of any kind to bully, harass, intimidate or attempt to radicalise others will not be tolerated, may amount to a criminal offence and will constitute a serious breach of discipline, whether or not you are in the care of the School at the time of such use. Appropriate disciplinary action will be taken where the School becomes aware of such use (see the School's anti-bullying policy (pupils) and behaviour and discipline policy) and the School's safeguarding procedures will be followed in appropriate circumstances (see the School's safeguarding and child protection policy).

10 Mobile electronic devices may be confiscated and searched in appropriate circumstances. Please see the policy on searching and the retention and disposal of confiscated items.

11 The School does not accept any responsibility for the theft, loss of, or damage to, mobile electronic devices brought onto School premises, including devices that have been confiscated or which have been handed in to staff.

Appendix 4 Photographs and images

1 Using photographic material of any kind to bully, harass or intimidate others will not be tolerated and will constitute a serious breach of discipline.

2 You may only use cameras or any mobile electronic device to take a still or moving image with the express permission of the member of staff in charge and with the permission of those appearing in the image. If the material found is a pornographic image of a child or an extreme pornographic image this will not be deleted and the device will be delivered to the police, as stated in paragraph 11.3 of this policy.

3 You must allow staff access to images stored on mobile phones and / or cameras and must delete images if requested to do so.

4 The posting of images which in the reasonable opinion of the School are considered to be offensive or which brings the School into disrepute on any form of social media or websites such as YouTube etc is a serious breach of discipline and will be subject to disciplinary procedures whatever the source of the material, irrespective of whether the image was posted using School or personal facilities.

5 **Sexting**

5.1 **Sexting** means the taking and sending or posting of images or videos of a sexual or indecent nature of you or another pupil, usually through mobile picture messages or webcams over the internet.

5.2 Sexting is strictly prohibited, whether or not you are in the care of the School at the time the image is recorded and / or shared.

5.3 Sexting may be a criminal offence, even if the picture is taken and shared with the permission of the person in the image. Even if you are not prosecuted, this may result in information being stored on your police record, which may prevent you from obtaining certain jobs in the future and may impact your freedom of travel.

5.4 The police may seize any devices which they believe may have been used for sexting. If the police find that a device contains inappropriate images, they are unlikely to return it to you.

5.5 Remember that once a photo or message is sent, you have no control about how it is passed on. You may delete the image but it could have been saved or copied and may be shared by others.

5.6 Images shared online become public and may never be completely removed. They could be found in the future by anyone, even by universities and future employers.

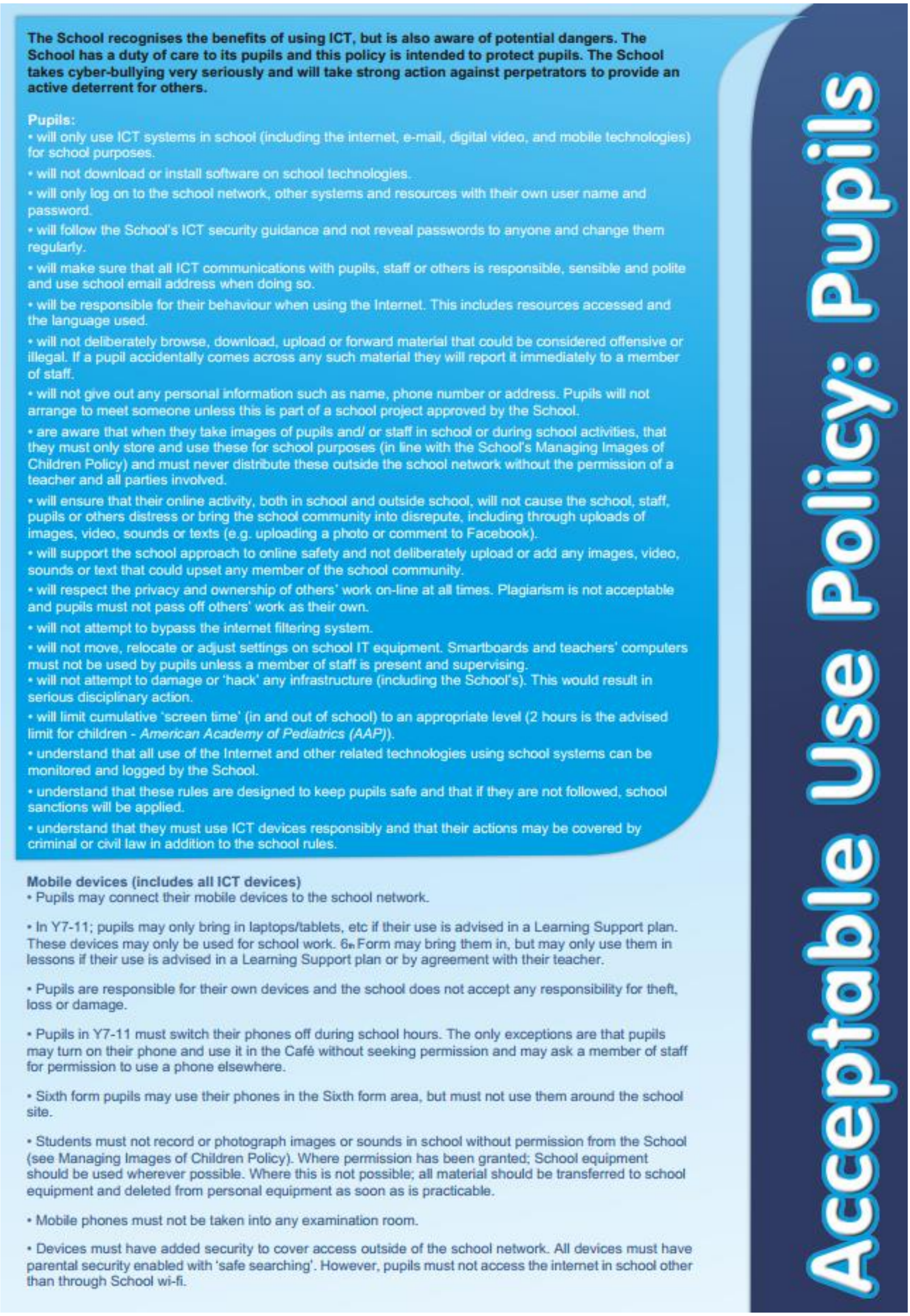
5.7 Even if you don't share images yourself, there is a risk that you may lose your device, it may be "hacked", or its data may still be accessible to a future owner.

5.8 The School will treat incidences of sexting (both sending and receiving) as a breach of discipline and also as a safeguarding matter under the School's child protection procedures (see the School's safeguarding and child protection policy).

5.9 If you are concerned about any image you have received, sent or forwarded or otherwise seen, speak to any member of staff for advice.

5.10 If sexual images or videos have been made and circulated online, you can be supported to get the images removed through the Internet Watch Foundation.

Appendix 5 ‘Pupil Friendly’ Poster



Acceptable Use Policy: Pupils

The School recognises the benefits of using ICT, but is also aware of potential dangers. The School has a duty of care to its pupils and this policy is intended to protect pupils. The School takes cyber-bullying very seriously and will take strong action against perpetrators to provide an active deterrent for others.

Pupils:

- will only use ICT systems in school (including the internet, e-mail, digital video, and mobile technologies) for school purposes.
- will not download or install software on school technologies.
- will only log on to the school network, other systems and resources with their own user name and password.
- will follow the School's ICT security guidance and not reveal passwords to anyone and change them regularly.
- will make sure that all ICT communications with pupils, staff or others is responsible, sensible and polite and use school email address when doing so.
- will be responsible for their behaviour when using the Internet. This includes resources accessed and the language used.
- will not deliberately browse, download, upload or forward material that could be considered offensive or illegal. If a pupil accidentally comes across any such material they will report it immediately to a member of staff.
- will not give out any personal information such as name, phone number or address. Pupils will not arrange to meet someone unless this is part of a school project approved by the School.
- are aware that when they take images of pupils and/ or staff in school or during school activities, that they must only store and use these for school purposes (in line with the School's Managing Images of Children Policy) and must never distribute these outside the school network without the permission of a teacher and all parties involved.
- will ensure that their online activity, both in school and outside school, will not cause the school, staff, pupils or others distress or bring the school community into disrepute, including through uploads of images, video, sounds or texts (e.g. uploading a photo or comment to Facebook).
- will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community.
- will respect the privacy and ownership of others' work on-line at all times. Plagiarism is not acceptable and pupils must not pass off others' work as their own.
- will not attempt to bypass the internet filtering system.
- will not move, relocate or adjust settings on school IT equipment. Smartboards and teachers' computers must not be used by pupils unless a member of staff is present and supervising.
- will not attempt to damage or ‘hack’ any infrastructure (including the School's). This would result in serious disciplinary action.
- will limit cumulative ‘screen time’ (in and out of school) to an appropriate level (2 hours is the advised limit for children - *American Academy of Pediatrics (AAP)*).
- understand that all use of the Internet and other related technologies using school systems can be monitored and logged by the School.
- understand that these rules are designed to keep pupils safe and that if they are not followed, school sanctions will be applied.
- understand that they must use ICT devices responsibly and that their actions may be covered by criminal or civil law in addition to the school rules.

Mobile devices (includes all ICT devices)

- Pupils may connect their mobile devices to the school network.
- In Y7-11; pupils may only bring in laptops/tablets, etc if their use is advised in a Learning Support plan. These devices may only be used for school work. 6th Form may bring them in, but may only use them in lessons if their use is advised in a Learning Support plan or by agreement with their teacher.
- Pupils are responsible for their own devices and the school does not accept any responsibility for theft, loss or damage.
- Pupils in Y7-11 must switch their phones off during school hours. The only exceptions are that pupils may turn on their phone and use it in the Café without seeking permission and may ask a member of staff for permission to use a phone elsewhere.
- Sixth form pupils may use their phones in the Sixth form area, but must not use them around the school site.
- Students must not record or photograph images or sounds in school without permission from the School (see Managing Images of Children Policy). Where permission has been granted; School equipment should be used wherever possible. Where this is not possible; all material should be transferred to school equipment and deleted from personal equipment as soon as is practicable.
- Mobile phones must not be taken into any examination room.
- Devices must have added security to cover access outside of the school network. All devices must have parental security enabled with ‘safe searching’. However, pupils must not access the internet in school other than through School wi-fi.