THE PERSE
SCHOOL
CAMBRIDGE

Acceptable Use of ICT Policy for Pupils

The Perse School

September 2023

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 potentially illegal, harmful or inappropriate content (such as pornographic, racist, extremist or offensive materials);

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

(c) inappropriate online contact or conduct, including sexual harassment;

(d) cyberbullying and other forms of abuse; and

(e) online challenges and online hoaxes.

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;

1.2.6 to prevent the unnecessary criminalisation of pupils; and

1.2.7 to help to promote 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 involves everyone in the School and seeks to ensure that the best interests of pupils underpins and is at the heart of all decisions, systems, processes and policies.

2 Scope and application

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

2.2 This policy applies to pupils using or accessing the School's technology whether on or off School premises, or using their own or others' technology in a way which affects the welfare of other pupils or any member of the School community or where the culture or reputation and orderly running of the School are put at risk.

2.3 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, 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 2023);

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

3.2.3 Sharing nudes and semi-nudes: advice for education settings working with children and young people (Department for Digital, Culture, Media & Sport (DfDCMS) and UK Council for Internet Safety (UKCIS), December 2020);

3.2.4 Relationships education, relationships and sex education and health education guidance (DfE, June 2019);

3.2.5 How can we stop prejudice based bullying in schools? (Equality and Human Rights Commission);

3.2.6 Safeguarding children and protecting professionals in early years settings: online safety considerations (UK Council for Internet Safety, February 2019);

3.2.7 Searching, screening and confiscation: advice for schools (DfE, September 2022): and

3.2.8 Behaviour in schools: advice for headteachers and school staff 2022 (DfE, September 2022).

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;

3.3.6 Relationships Education and Relationships and Sex Education Policy;

3.3.7 Risk Assessment Policy For Pupil Welfare;

3.3.8 Inclusion Equality and Diversity Policy; and

3.3.9 Preventing Extremism and Radicalisation Policy.

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.

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

5.2 The School will take a wide and purposive approach to considering what falls within the meaning of technology, networks and devices used for views or exchanging information (collectively referred to in this policy as **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 and school messaging platforms including Microsoft Teams, and Schoology;

5.2.3 generative artificial intelligence technology/tools;

5.2.4 electronic communications;

5.2.5 mobile phones and smart technology;

5.2.6 wearable technology;

5.2.7 desktops, laptops, netbooks, tablets / phablets, chromebooks;

5.2.8 personal music players;

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

5.2.10 social networking, micro blogging and other interactive websites;

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

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

5.2.13 gaming sites;

5.2.14 virtual learning environments (such as Microsoft Teams);

5.2.15 SMART boards, display screens;

5.2.16 other photographic or electronic equipment e.g. GoPro devices; and

5.2.17 devices which allow sharing services offline (such as Apple's AirDrop).

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	Upper School - Deputy Head (Pupil development and welfare) Prep School - Deputy Head Pelican School - Head Director of ICT	As required, and at least annually
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, 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 Head Director of ICT	As required, and at least termly
Online safety	Designated Safeguarding Lead	As required, and at least annually
Maintaining up to date records of all information created in relation to the policy and its implementation as required by the UK GDPR	Director of ICT	As required, and at least termly

Task	Allocated to	When / frequency of review
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. Staff are aware that technology can be a significant component in many safeguarding and wellbeing issues and 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://mysafetynet.org.uk/

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

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

7.4 Please see the School's *Online Safety Policy* for further information about the School's online safety strategy.

8 Internet and email/electronic communication systems

8.1 The School provides internet, intranet access and, in Year 3 and above, an email/electronic communication 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/electronic communication systems. If a pupil is unsure about whether they are doing the right thing, they must seek assistance from a member of staff. Pupils are given individual user names and passwords to access the School's internet, intranet and email system and these details must not be disclosed to any other person.

8.3 The use of any device connected to the School's network will be logged and monitored by the ICT Department.

8.4 For the protection of all pupils, their use of email/electronic communication and of the internet will be monitored by the School. Pupils should remember that even when an email/electronic message 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 communicating on or off-line using devices, apps, platforms and email (Appendix 2);

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

9.1.4 photographs and images (including the consensual and non-consensual sharing of nude and semi-nude images and videos (Appendix 4).

These rules are condensed into 'pupil-friendly' posters displayed in appropriate locations in the School, and in the Acceptable Use Agreement contained in the Prep School planner (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 in school and at home, whether during or outside School.

10 Procedures

10.1 The way in which pupils relate to one another online can have significant impact on the School's culture. Pupils are responsible for their actions, conduct and behaviour when using technology at all times. Even though online space differs in many ways, the same standards of behaviour are expected online as apply offline. Use of technology should be safe, responsible and respectful to others and legal. If a pupil is aware of misuse by other pupils they should talk to a teacher about it immediately.

10.2 Any misuse of technology by pupils will be dealt with under the School's *Behaviour and Discipline Policy*. Incidents involving the misuse of technology which are considered to be of a safeguarding nature will be dealt with in accordance with the School's *Safeguarding and Child Protection Policy* and procedures, rather than 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, including cyberbullying, prejudiced-based bullying and discriminatory bullying, 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 School has adopted a zero tolerance approach to sexual violence and sexual harassment - it is never acceptable and it will not be tolerated. Incidents of sexual violence or sexual harassment will not be dismissed as merely "banter" or "just having a laugh" or "boys being boys" as this can lead to the creation of a culture of unacceptable behaviours and an unsafe environment for children and, in worst case scenarios, a culture that normalises abuse.

10.5 Sexual harassment, in the context of this policy, means "unwanted conduct of a sexual nature" and the School recognises that this can occur both online and offline. Pupils must not therefore use their own or the School's technology to sexually harass others at any time, whether during or outside of school. Incidents of sexual harassment involving the use of technology will be dealt with under the School's behaviour and discipline and safeguarding policies. If a pupil thinks that they might have been sexually harassed or that another person is being sexually harassed, they should talk to a teacher about it as soon as possible.

10.6 The School recognises that children's sexual behaviour exists on a wide continuum ranging from normal and developmentally expected to inappropriate, problematic, abusive and violent. Problematic, abusive and violent sexual behaviour is developmentally inappropriate and may cause developmental damage. Such behaviour can be classed under the umbrella term "harmful sexual behaviour" and the School is award that this can occur online and/or face-to-face and can also occur simultaneously between the two.

10.7 Any reports of sexual violence or sexual harassment will be taken extremely seriously by the School and those who have been victim to such abuse will be reassured, supported and kept safe throughout. No pupil should ever be made to feel that they have created a problem or feel ashamed for reporting their concern. Pupils should be aware that teachers may not be able to provide an assurance of confidentially in relation to their concern as information may need to shared further (e.g. with the School's Designated Safeguarding Lead) to consider next steps. See Appendix 6 for further information.

10.8 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 member of staff about it as soon as possible.

10.9 The School is also aware of the risks of radicalisation and understands that this can occur through many different methods (including social media or the internet. In a case where the pupil is considered to be vulnerable to radicalisation they may be referred to the Channel programme in accordance with the School's *Safeguarding and Child Protection Policy*. 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).

10.10 Cybercrime:

10.10.1 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).

10.10.2 Cyber-dependent crimes include:

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

(b) 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

(c) Making, supplying or obtaining malware (malicious software) such as viruses, spuware, ransomeware, botnets and Remote Access Trojans with the intent to commit further offences, including those above.

10.10.3 The School is aware that pupils with particular skill and interest in computing and technology may inadvertently or deliberately stray into cybercrime.

10.10.4 Any concerns about a pupil in this area will be referred to the Designated Safeguarding Lead immediately. The Designated Safeguarding Lead will 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.

10.11 In addition to following the procedures in the relevant policies as set out above, all serious incidents involving technology must be reported to the Upper School Deputy Head (Pupil development and welfare), Prep School Deputy Head, Pelican School Head or the Director of ICT who will record the matter centrally in the technology incidents log.

11 Generative Artificial Intelligence

11.1 The School recognises the increasing presence of generative artificial intelligence (AI) technology. Although generative AI is not new, recent advances mean this technology is easily available to pupils to produce AI-generated content such as test, audio, code, images and video simulations.

11.2 When using any generative AI technologies pupils are expected to consider the following:

11.2.1 AI and human intelligence are not the same: AI tools do not understand what they produce or the impact the generated content may have;

11.2.2 sometimes AI tools will generate answers that sound plausible but they may not be correct;

11.2.3 content produced may perpetrate harmful biases and stereotypes and may not be age-appropriate;

11.2.4 over-reliance on these tools will reduce opportunities to improve research skills, writing and critical thinking;

11.2.5 AI tools store and learn information submitted to them so personal or sensitive information should never be entered;

11.2.6 if teachers indicate that pupils are permitted to use generative AI technologies in their work, pupils must observe all related instructions and guidance; and

11.2.7 submitting work produced in whole or part by AI without proper referencing or acknowledging using AI may be considered cheating and inappropriate use of AI.

11.3 Any misuse or inappropriate use of AI technologies by pupils will be addressed in accordance with the School's *behaviour and discipline policy* and disciplinary procedures.

11.4 The School may implement measures to ensure the safe and appropriate use of AI technologies within its network. These measures may include monitoring AI activities, restricting access to certain AI systems, or providing guidelines and restrictions on the use of specific AI applications.

12 Sanctions

12.1 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. Any action taken will depend on the seriousness of the offence.

12.2 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 Annex 5 (Searching and Confiscation) of the School's *Behaviour and Discipline Policy.*

12.3 If there are reasonable grounds to suspect that the confiscated device contains evidence in relation to an offence e.g. upskirting, 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.

12.4 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.

13 Training

13.1 The School ensures that regular guidance and training is arranged on induction and at regular intervals thereafter so that staff, including supply staff, and volunteers;

13.1.1 understand what is expected of them by this policy;

13.1.2 have the necessary knowledge and skills to carry out their roles; and

13.1.3 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.

13.2 Staff training is regularly updated and ongoing staff development training includes (but is not limited to) training on technology safety together with specific safeguarding issues including sharing nudes and semi-nudes images and / or videos, cyberbullying, radicalisation and dealing with harmful online challenges and online hoaxes. This training may be in addition to the regular safeguarding and child protection (including online safety) updates are required at induction and at least annually thereafter.

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

13.4 The School maintains written records of all staff training.

14 Risk Assessment

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

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

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

14.4 The Upper School Head, Prep School Head or Pelican School Head, as appropriate, has overall responsibility for ensuring that matters which affect pupil welfare in each school are adequately risk assessed and for ensuring that the relevant findings are implemented, monitored and evaluated.

14.5 Day to day responsibility to carry out risk assessments under this policy will be delegated to the Director of ICT, who is tasked with carrying out the particular assessment.

15 Record keeping

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

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

15.3 The information created in connection with this policy may contain personal data. The School's use of this 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 is set out in the School's data protection policies and procedures. 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*.

16 Version control

Date of adoption of this policy	6th September 2023
Date of last review of this policy	August 2023
Date for next review of this policy	August 2024
Policy owner (SMT)	Director of ICT
Authorised by	Jonathan Scott On behalf of the Board of Governors
Circulation	Governors / teaching staff / all staff / all parents / Upper pupils Published on the School's website and Perse Portal and available from the School Office on request

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 BYOD laptop, other mobile electronic device connected to the School’s wifi or the middle school managed devices used in school and away from school are covered by this policy regarding acceptable behaviour.

4 The use of cellular data (e.g. GPRS, 3G, 4G, 5G 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 that appropriate security and filtering is enabled on their child’s device.

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 user account or to confidential information to which you are not authorised to access. If there is a problem with your passwords, you should speak to a member of staff 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 security hardware and software 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 security hardware or software must be reported to a member of staff or the Director of ICT.

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 and malware can cause serious harm to the security of the School's network and that of others. Viruses and malware 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 or malware, 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, anti-malware or pupil-monitoring software on the School's computers including the middle school devices issued to pupils in Y9-11.

12 The use of location services can represent 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/electronic communication services

1 The School does not undertake to provide continuous internet access. Email/ electronic communication services 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 breach copyright or plagiarise (pass off as your own) another's work.

4 You must not load material from any external storage device brought in from outside the School onto the School's systems, unless this has been authorised by the Director of ICT.

5 You must not view, retrieve, download or share any illegal, offensive, potentially harmful or inappropriate material. Such material includes, but is not limited to, content that is abusive, racist, considered to be of an extreme or terrorist related nature, sexist, misogynistic/misandrist, homophobic, biphobic, pornographic, defamatory or that relates to any form of bullying or sexual violence/sexual harassment 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.

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

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

Use of email/electronic communication services

8 Your School email/electronic communication accounts can be accessed using personal devices (home desktop or laptop) by going to https://portal.office.com. You can also use the Microsoft Outlook App on a smartphone to sync School emails. Instructions are available from the ICT Office.

9 You must use your School email/electronic communication accounts e.g. the chat functionality of Microsoft Teams, virtual learning environment, homework submission tool etc as the only mean(s) of electronic communication with staff. Communication either from a personal email account or to a member of staff's personal email/electronic communication account is not permitted.

10 Email/electronic communications should be treated in the same way as any other forms of written communication. You should not include or ask to receive anything in a message 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 messages could be forwarded to or seen by someone you did not intend.

11 You must not send or search for any messages which contain illegal, offensive, potentially harmful or inappropriate material. Such material includes, but is not limited to, content that

is abusive, racist, considered to be of an extreme or terrorist related nature, sexist, misogynistic/misandrist, homophobic, biphobic, pornographic, indecent, defamatory or that relates to any form of bullying or sexual violence/sexual harassment 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/electronic communication system in this way is a serious breach of discipline and may constitute a criminal offence.

12 Trivial messages and jokes should not be sent or forwarded through the School's email/electronic communication 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.

13 You must not use the School's email / electronic communication systems to send misogynistic messages or messages which contain language relating to sexual violence or which could be interpreted as being harassment, whether of a sexual nature or otherwise. The School has adopted 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.

14 All correspondence from your School email/electronic communication account must contain the School's disclaimer.

15 You must not read anyone else's emails/electronic communication without their consent.

Other online communication (including social media, Schoology, Zoom (chats) and Microsoft Teams)

16 Anything you post online whether through messaging, social media or by other means needs to be considered carefully. Remember that there is a ‘disinhibition effect’ making you more likely to post things you might regret. The School may become involved in anything between members of the school community or that may bring the school into disrepute. Private conversations are rarely private and should not be considered so.

17 Only post messages or images you would be happy for a teacher, parent or guardian to see. Avoid making strongly opinionated comments which could be deemed offensive. Avoid making comments related to protected characteristics.

18 Anonymous posting is unwise. If pupils set up accounts to post anonymously (or that the presence of a group allows anonymity) all members of the group will be deemed individually responsible for material posted unless an individual admits responsibility. Nevertheless, other members of the group will be deemed partially responsible unless they have reported inappropriate posts or actively attempted to dissuade the perpetrator.

19 Do not make comments about individuals or the school online. They may be your views, but they could cause offence and the internet is not the place for such comments.

20 Never pose as anyone else or any institution.

21 Do not harass others or post things intended to upset them. Do not troll.

22 Some messages and images may seem to be temporary and permanently deleted – this may

not be the case if screenshots or photos are taken. Treat all posts as permanent.

23 Be cautious of meeting someone you meet online in real life. Always take an adult with you and tell people where you are going and who you are meeting.

24 Remember: once you share something it can be freely and easily copied, shared or manipulated. Once you've shared it – you've lost control of it.

25 Don't use ICT in your bedroom as it affects sleep and can make it more likely that you will post something you will regret. It is also best to avoid using ICT when tired. Switch off an hour before bed time and leave devices out of the bedroom.

26 Consider how much ICT you use in a day. Use of the internet and gaming can both be addictive and it is difficult to self-regulate use.

27 Be careful not to believe all you read online. Some sites publish dangerously inaccurate material. Be especially careful when investigating health concerns, sexuality and identity and searching for supportive communities.

Appendix 3 Use of mobile electronic devices and smart technology

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

2 At 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 permitted in designated locations (PAC Café, Library and Sixth form area) or with express permission from a member of staff for a specific purpose and time.

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

4 Pupils at the Prep School may not bring mobile phones to school unless required for travelling to school independently. 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 The School does all that is reasonably can to limit pupils' exposure to potentially harmful and inappropriate material online through the use of the School's IT system. The School has appropriate filtering and monitoring systems in place to protect pupils using the internet (including email, messaging and social media sites) when connected to the School's network, and their effectiveness is regularly reviewed.

6 The School acknowledges that many pupils will have unlimited and unrestricted access to the internet via mobile phone networks (i.e. 3G, 4G and 5G) and is aware that this means that some children, whilst at School, may sexually harass, bully, and control others via their mobile and smart technology, share indecent images consensually and non-consensually (often via large chat groups) and view and share pornography and other harmful content.

7 The use of cellular data (e.g. GPRS, 3G, 4G, 5G etc) to access the internet while pupils are on School premises or otherwise in the care of the School is discouraged, 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.

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

9 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.

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

11 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.

12 Use of electronic devices of any kind to bully, harass, intimidate or attempt to radicalise others or to share indecent images: consensually and non-consensually (including in large chat groups) or to view and share pornography and other harmful or potentially harmful or inappropriate content 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*).

13 Pupils must not use their mobile and smart technology to send racist, sexist, homophobic, biphobic, pornographic, indecent, defamatory, misogynistic/misandrist messages or messages which contain language relating to sexual violence or which could be interpreted as being harassment, whether of a sexual nature or otherwise, or considered to be of an extreme or terrorist related nature. The School has adopted 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. Pupils are encouraged to report inappropriate messages to a trusted adult.

14 Devices connected to the School’s network are logged and monitored (see paragraph 8.3 of the main policy

15 Mobile electronic devices may be confiscated and searched in appropriate circumstances. Please see the Annex 5 (Searching and Confiscation) of the School’s *Behaviour and Discipline Policy*.

16 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.

3 You must allow staff access to images stored on mobile phones and / or cameras and must delete images if requested to do so. 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 12.3 of this policy.

4 If material found on a device is a still or moving image that has been obtained by 'upskirting' this will not be deleted and the device will be delivered to the police, as stated in paragraph 12.3 of this policy.

5 You must allow staff access to images stored on mobile phones and / or cameras and must delete images if requested to do so. Staff will not view or forward illegal images of children.

6 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, 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.

7 **Sharing nude and semi-nude images and videos**

7.1 "Sharing nudes and semi-nudes" means the consensual and non-consensual taking and sending or posting of nude or semi-nude images, videos or live streams by young people under the age of 18 online. This could be via social media, gaming platforms, chat apps or forums. It can also involve sharing between devices offline e.g. via Apple's AirDrop. This may also be referred to as sexting or youth produced sexual imagery.

7.2 Sharing or soliciting sexual images is strictly prohibited, whether or not you are in the care of the School at the time the image is recorded and / or shared.

7.3 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.

7.4 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.

7.5 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.

7.6 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.

7.7 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.

7.8 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*).

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

7.10 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.

8 Upskirting

8.1 Upskirting typically involves taking a picture under a person's clothing without their permission and/or knowledge, with the intention of viewing their genitals or buttocks (with or without underwear) to obtain sexual gratification, or cause the victim humiliation, distress or alarm.

8.2 Upskirting is strictly prohibited, whether or not you are in the care of the School at the time the image is recorded.

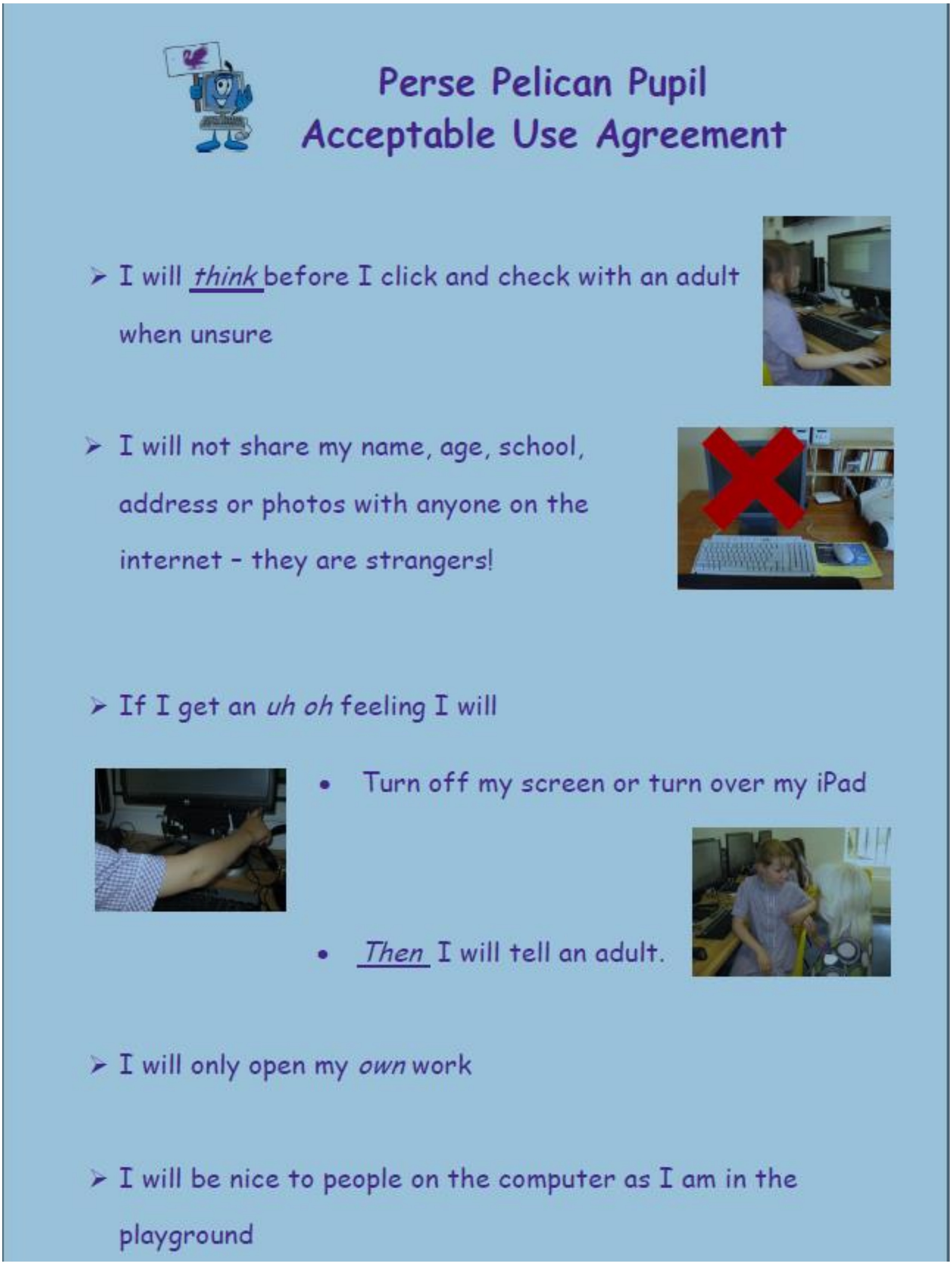
8.3 Upskirting is a criminal offence. Attempting to commit an act of upskirting may also be a criminal offence e.g. if actions are taken to do something that is more than merely preparatory to committing the offence such as attempting to take a photograph on a telephone or camera but failing to do so because of lack of storage space or battery.

8.4 The School will treat incidences of upskirting 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*).

8.5 If you are concerned that you have been a victim of upskirting, speak to any member of staff for advice.

Appendix 5 ‘Pupil Friendly’ Posters

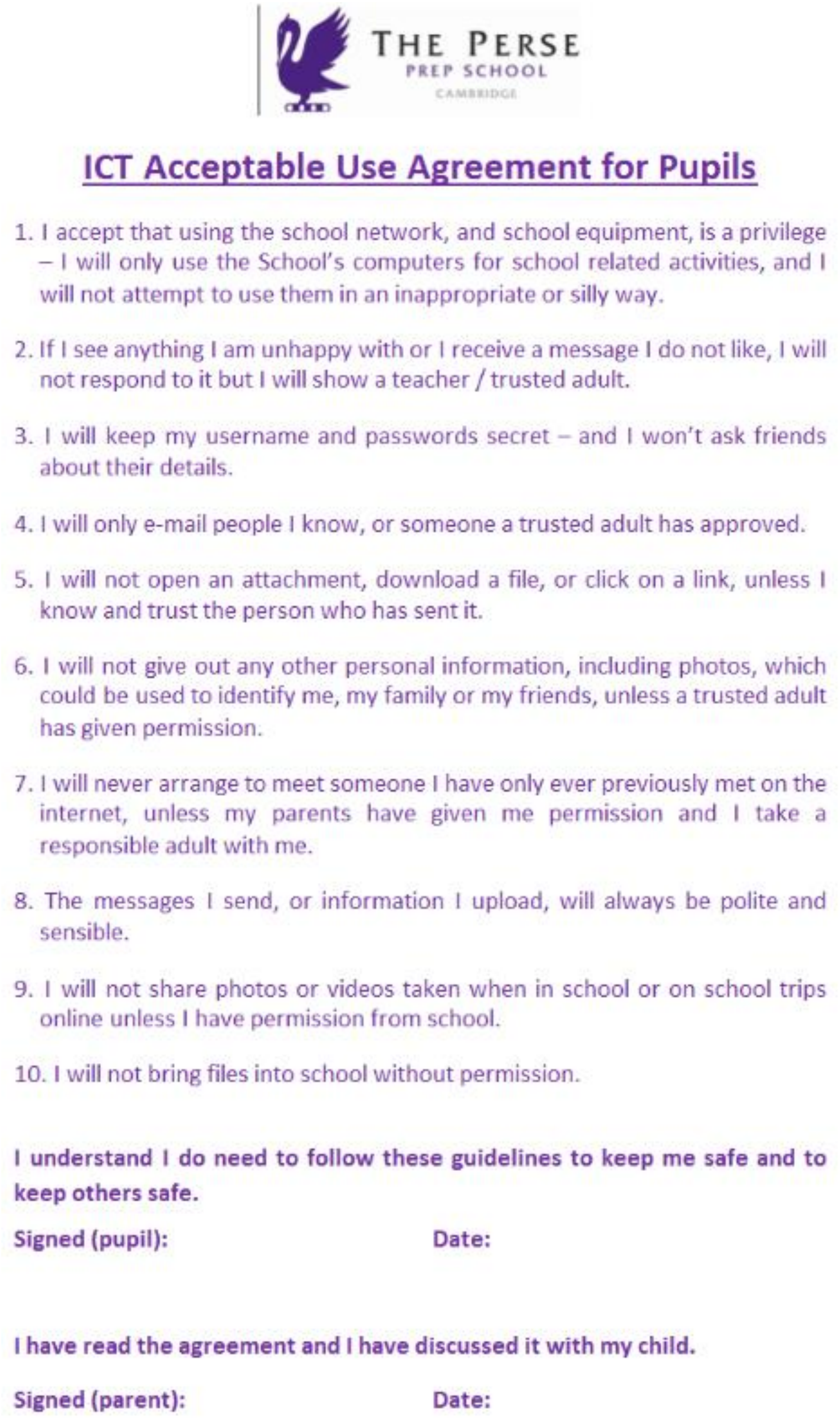
Pelican School Poster



Perse Pelican Pupil
Acceptable Use Agreement

- I will *think* before I click and check with an adult when unsure
- I will not share my name, age, school, address or photos with anyone on the internet – they are strangers!
- If I get an *uh oh* feeling I will
  - Turn off my screen or turn over my iPad
  - *Then* I will tell an adult.
- I will only open my *own* work
- I will be nice to people on the computer as I am in the playground

Prep School Planner page



THE PERSE
PREP SCHOOL
CAMBRIDGE

ICT Acceptable Use Agreement for Pupils

1. I accept that using the school network, and school equipment, is a privilege – I will only use the School's computers for school related activities, and I will not attempt to use them in an inappropriate or silly way.

2. If I see anything I am unhappy with or I receive a message I do not like, I will not respond to it but I will show a teacher / trusted adult.

3. I will keep my username and passwords secret – and I won't ask friends about their details.

4. I will only e-mail people I know, or someone a trusted adult has approved.

5. I will not open an attachment, download a file, or click on a link, unless I know and trust the person who has sent it.

6. I will not give out any other personal information, including photos, which could be used to identify me, my family or my friends, unless a trusted adult has given permission.

7. I will never arrange to meet someone I have only ever previously met on the internet, unless my parents have given me permission and I take a responsible adult with me.

8. The messages I send, or information I upload, will always be polite and sensible.

9. I will not share photos or videos taken when in school or on school trips online unless I have permission from school.

10. I will not bring files into school without permission.

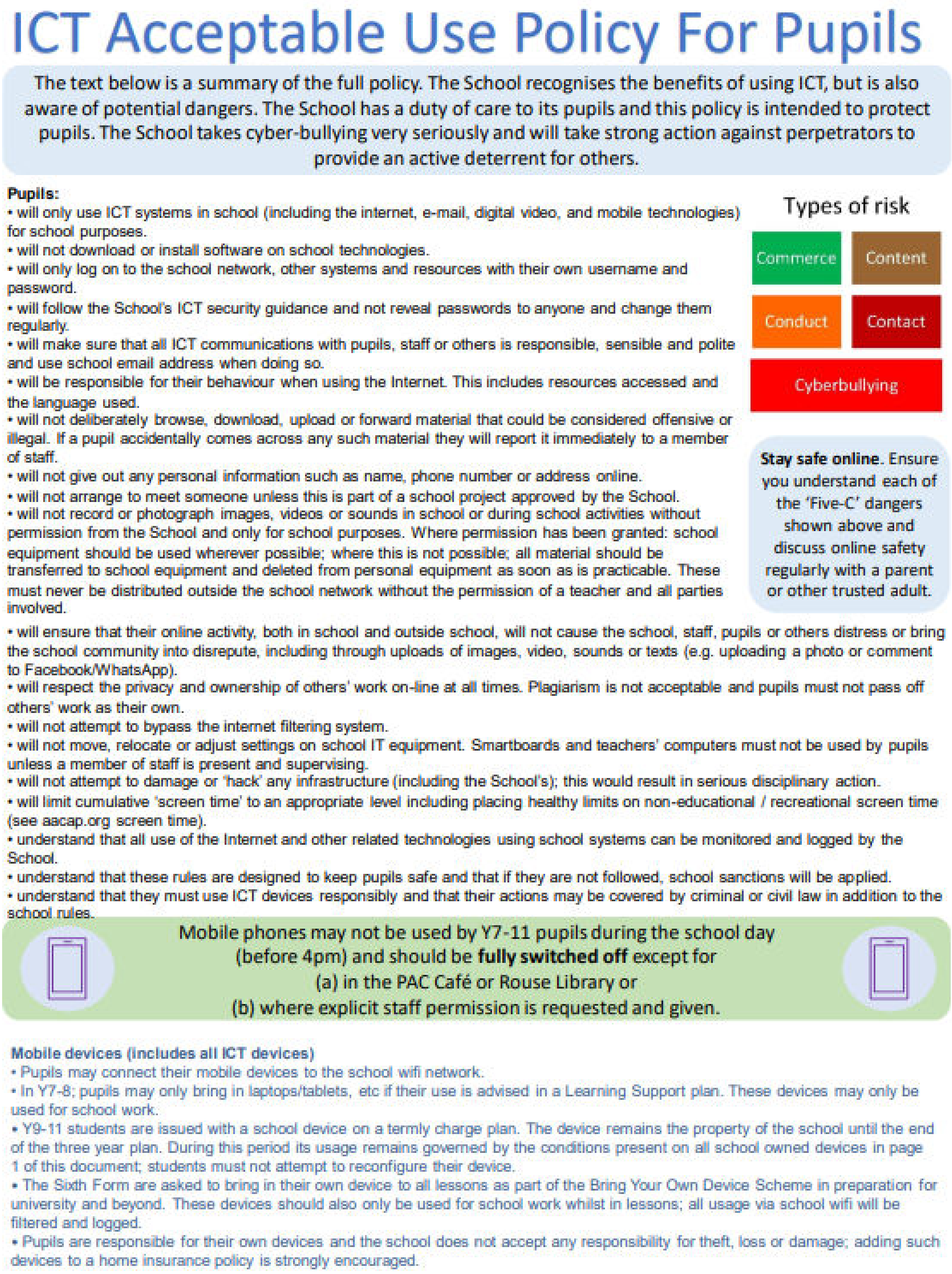
I understand I do need to follow these guidelines to keep me safe and to keep others safe.

Signed (pupil): **Date:**

I have read the agreement and I have discussed it with my child.

Signed (parent): **Date:**

Upper School Poster



ICT Acceptable Use Policy For Pupils

The text below is a summary of the full policy. 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 username 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 online.
- will not arrange to meet someone unless this is part of a school project approved by the School.
- will not record or photograph images, videos or sounds in school or during school activities without permission from the School and only for school purposes. 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. These must never be distributed 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/WhatsApp).
- 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' to an appropriate level including placing healthy limits on non-educational / recreational screen time (see aacap.org screen time).
- 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.

Types of risk

Commerce	Content
Conduct	Contact
Cyberbullying	

Stay safe online. Ensure you understand each of the 'Five-C' dangers shown above and discuss online safety regularly with a parent or other trusted adult.

Mobile phones may not be used by Y7-11 pupils during the school day (before 4pm) and should be **fully switched off** except for
(a) in the PAC Café or Rouse Library or
(b) where explicit staff permission is requested and given.

Mobile devices (includes all ICT devices)

- Pupils may connect their mobile devices to the school wifi network.
- In Y7-8; 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.
- Y9-11 students are issued with a school device on a termly charge plan. The device remains the property of the school until the end of the three year plan. During this period its usage remains governed by the conditions present on all school owned devices in page 1 of this document; students must not attempt to reconfigure their device.
- The Sixth Form are asked to bring in their own device to all lessons as part of the Bring Your Own Device Scheme in preparation for university and beyond. These devices should also only be used for school work whilst in lessons; all usage via school wifi will be filtered and logged.
- Pupils are responsible for their own devices and the school does not accept any responsibility for theft, loss or damage; adding such devices to a home insurance policy is strongly encouraged.

Appendix 6 Online sexual harassment

1 Online sexual harassment means "unwanted conduct of a sexual nature" occurring online, whether in School or outside of it.

2 The School takes a zero tolerance approach to online sexual harassment and it is never acceptable and it will not be tolerated. The School will treat 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 child protection procedures (see the School's *Safeguarding and Child Protection Policy* and procedures).

3 All allegations will be responded to seriously and all victims will be reassured and offered appropriate support, regardless of how long it has taken for them to come forward, and kept safe.

4 The School will consider online sexual harassment in broad terms, recognising that it can occur between two or more children of any age or sex and through a group of children sexually harassing a single child or group of children.

5 It will consider whether incidents of online sexual harassment are standalone, or part of a wider pattern of sexual harassment and / or sexual violence. It may include:

5.1 consensual and non-consensual sharing of nude and semi-nude images and/or videos and sexual images;

5.2 the sharing of unwanted explicit content;

5.3 sexualised online bullying;

5.4 unwanted sexual comments and messages, including on social media;

5.5 sexual exploitation, coercion or threats; and

5.6 coercing others into sharing images of themselves or performing acts they’re not comfortable with online.

6 If you are concerned that you have been a victim of online sexual harassment, speak to any member of staff for advice.

7 When dealing with online sexual harassment staff will follow the *School's Safeguarding and Child Protection Policy* and procedures.

8 The Head and staff authorised by them have a statutory power to search pupils / property on school premises. This includes content of mobile phones and other devices if there is reasonable suspicion that a device contains illegal or undesirable material relating to online sexual harassment. The school's search procedures can be found in the School's *Behaviour and Discipline Policy*.

Appendix 7 Harmful online challenges and online hoaxes

1 A hoax is a deliberate lie designed to seem truthful, and online challenges generally involve users recording themselves taking a challenge or following a trend, and then distributing the video through social media channels, inspiring or daring others to repeat the challenge.

2 If the School becomes aware that harmful online challenges or online hoaxes are circulating between pupils, the School will handle this as a safeguarding matter under the School's child protection procedures (see the School's *Safeguarding and Child Protection Policy* and procedures).

3 The DSL will take a lead role in assessing the risk to the School community, undertake a case-by-case assessment, including considering if the risk is a national one or localised to the area, or just the School.

4 The factual basis of any harmful online challenge or online hoax will be checked through known reliable and trustworthy sources e.g. the Professional Online Safety Helpline, local safeguarding partners or local police force.

5 If, following investigation, the DSL finds that pupils have deliberately shared information with the intention of encouraging others to participate in harmful online challenges or online hoaxes, this will be treated as a breach of discipline and will be dealt with under the School's *Behaviour and Discipline Policy*.

6 The Headteacher and staff authorised by them have a statutory power to search pupils / property on school premises. This includes content of mobile phones and other devices if there is reasonable suspicion that a device is being used to commit an offence or cause personal injury or damage to property. The School's search procedures can be found in the *Behaviour and Discipline Policy*

Appendix 8 Middle School Devices

1. Middle School devices, owned by the School are issued to pupils in Years 9 – 11. At the end of Year 11, ownership of the devices will be transferred to the pupil/parent.

2. The device is supplied with a rubber-edged case. The school has an excess charge for device repairs so long as rubber case protection is in place. If the rubber edging becomes damaged at any point, pupils should go to the ICT office for a replacement immediately. If the rubber-edge protection is not in place and the device is damaged, parents may have to pay the total repair cost, not just the excess.

3. ALL internet browsing, whether on site or at home, goes through the school filtering service. Regular reports of filtering blocks will lead to ICT & pastoral investigations during which time devices will be removed from students and, in conjunction with parental discussion, devices may be retained for a longer time if pupils cannot be trusted to use devices safely and purposefully. For this reason there should be clear separation at all times with school devices used for school related and educational activities. Devices should not be used, for example, to stream sport on unofficial/illegal sites which often generate safety-filtering alerts which ICT will then pass on to the pastoral team due to inappropriate adverts being blocked.

4. Pupils must not install any additional software without specific permission from a member of staff which will only be given for educational related applications or for minor accessories such as spotify. Failure to observe this may result in a device suspension; the ICT team routinely run software installation queries to check what software is active on Surface devices.

5. Pupils are responsible for the device in school, at home and when out and about. Pupils are required to take appropriate care for the device, similar to how you look after a personal device such as a phone or personal laptop. For example:

   Bags containing devices must <u>never</u> be left on the floor around the site; pupils must <u>always</u> use one of the many bag racks located all around the site. Bags can easily get accidentally trodden on if left exposed, breaking the screen. Similarly, in classrooms, bags should be placed safely under desks.

   When out and about, devices must never be left unattended and should be on your person at all times.

   Devices should not be left in vehicles overnight, locked or unlocked.

6. If the device is damaged, lost or stolen, please report it to the IT Office immediately in person or via email (ictsupport@perse.co.uk)