ROEDEAN

POLICY TITLE	**ICT Acceptable Use Policy for Pupils**

Policy Area	Safeguarding
Author	MC
Relevant Statutory Regulations	Education (Independent School Standards) Regulations 2014 National minimum standards for boarding schools (Department for Education (DfE), September 2022) Education and Skills Act 2008 Children Act 1989 Data Protection Act 2018 and UK General Data Protection Regulation (UK GDPR) Equality Act 2010 Keeping Children Safe in Education (KCSIE 2023)
Senior Team Lead	Director of Finance and Administration
Version	2022.1
Last Updated	October 2022
Review Date	**October 2023**

Contents

Appendix

1 Aims

1.1 This is the acceptable use policy for pupils of Roedean School (**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 openness, safety, equality and protection.

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

2 Scope and application

2.1 This policy applies to the whole School community, including boarders.

2.2 This policy applies to pupils 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 of the School is put at risk.

2.3 This policy and the acceptable use documents for ICT for pupils applies to all technology fully or partially owned or operated by Roedean School and to any computer used on its premises whether or not connected to the school network. This includes:

2.3.1 The voice and data networks that connect them.

2.3.2 All devices connected to these computers and networks.

2.3.3 The hardware and software associated with these systems.

2.3.4 The information managed by these systems.

2.4 Additional rules on the use of technology in boarding houses is provided in the Boarders' Handbook.

2.5 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 National minimum standards for Boarding Schools (Department for Education (**DfE**), September 2022);

3.1.3 Education and Skills Act 2008;

3.1.4 Children Act 1989;

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) (**KCSIE**);

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

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

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

3.2.7 Relationships education, relationships and sex education and health education guidance (DfE, September 2021).

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

3.3.1 promoting good behaviour policy;

3.3.2 preventing and tackling bullying policy;

3.3.3 online safety policy;

3.3.4 exclusions policy

3.3.5 child protection and safeguarding policy and procedures;

3.3.6 risk assessment policy for pupil welfare;

3.3.7 relationships and sex education (RSE) policy

3.3.8 school rules

4 Publication and availability

4.1 This policy is published on the School website.

4.2 This policy is available in hard copy on request.

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

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

5 Definitions

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

5.1.1 References to the **Proprietor** are references to the Council of Roedean School.

5.1.2 Reference 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 viewing 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;

5.2.3 electronic communications;

5.2.4 mobile phones and smart technology;

5.2.5 wearable technology;

5.2.6 desktops, laptops, netbooks, tablets / phablets;

5.2.7 personal music players;

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

5.2.9 social networking, micro blogging and other interactive websites;

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

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

5.2.12 gaming sites;

5.2.13 virtual learning environments such as SharePoint;

5.2.14 SMART boards;

5.2.15 other photographic or electronic equipment (e.g. GoPro device); and

5.2.16 devices which allow sharing services offline (e.g. Apple's AirDrop).

6 Responsibility statement and allocation of tasks

6.1 The Proprietor 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 Proprietor 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	IT Manager	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	IT Manager	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	IT Manager	As required, and at least annually
Online safety	Designated Safeguarding Lead	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	IT Manager Deputy Head: Pastoral	As required, and at least annually
Formal annual review	Proprietor	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 and many of its policies and procedures. 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 Use of personal electronic devices

7.3.1 Pupils are responsible for their own belongings. The school accepts no responsibility for replacing property that is lost, stolen or damaged either at school or travelling to and from school.

7.3.2 Pupils are responsible for replacing lost or damaged school property, including electronic devices.

7.3.3 Parents must be aware if their child takes a personal device including mobile phone, tablet or laptop to school.

7.3.4 Personal electronic devices will be switched off and kept out of sight during lessons, unless the pupil is using the device as part of a lesson with the permission of their class teacher.

7.3.5 In years 7-10, mobile phones will be handed in to Heads of Year on arrival into school and returned at the end of the day. For Year 11-13, mobile phones may only be used for voice calls in emergency situations and with the express permission of a member of staff.

7.3.6 Outside lessons, pupils in years 11-13 should have their phones on silent or switched off. Mobile phones should not be used in communal settings and should be kept out of sight in dining rooms and in co-curricular activities, assemblies, house meetings and so on unless express permission is given by a member of staff.

7.3.7 All pupils are expected to sign the Pupil Personal Electronic Devices Agreement (Appendix 9) and confirm they understand what is expected with regard to the use of personal devices.

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

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

7.4.2 https://www.childnet.com/young-people

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

7.4.4

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

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

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

7.4.8 https://www.gov.uk/government/publications/indecent-images-of-children-guidance-for-young-people/indecent-images-of-children-guidance-for-young-people

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

7.6 Please see Appendix 6 for details of the School's response to online challenges and hoaxes.

8 Internet and email / electronic communication systems

8.1 The School provides internet, intranet and social media access and an email / electronic communication system (Microsoft Outlook / Microsoft Teams) to pupils to support their academic progress and development. Pupils are given individual usernames and passwords to access the School's internet, intranet and email system and these details must not be disclosed to any other person.

8.2 Pupils may only access the School's network when given specific permission to do so. All pupils will receive guidance on the use of the School's internet and 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.

8.3 No laptop or other mobile electronic device may be connected to the School network without use of your school log on credentials. The use of any device connected to the School's network will be logged and monitored by the ICT team.

8.4 For the protection of all pupils, their use of email / electronic communication system 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. The School uses several systems such as Filtering, Anti-Malware and Firewalls to protect and monitor internet access. [see Appendix 3].

9 School rules

9.1 Pupils **must** be aware of and observe rules and principles set out in the following Appendices:

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);

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

9.1.5 online sexual harassment (Appendix 5); and

9.1.6 harmful online hoaxes and challenges (Appendix 6).

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, whether during or outside of school.

10 Guidance for Acceptable Internet Use

10.1 The internet, primarily, is provided for pupils to conduct research and back-up their work. Access is a privilege, not a right and that access requires responsibility. Individual users of the internet are responsible for their behaviour and communications over the network. Users must comply with school standards and honour the agreements they have signed.

10.2 During periods of online learning, pupils and parents will sign codes of conduct and consent forms and these can be found as appendices 7 and 8.

10.3 Pupils must not give personal information to anyone on the internet or by e-mail and they must not view, upload or download, or send by email, any material which may infringe copyright, any other Intellectual Property or is likely to be unsuitable for children or the School. This applies to any offensive material which includes but is not limited to material of a violent, dangerous, abusive, or racist nature or containing inappropriate sexual content, considered to be of an extreme or terrorist nature, sexist, homophobic, any form of bullying, pornographic or criminal activity. If they are unsure, they must ask a teacher.

10.4 Staff may review files and communications to ensure that users are using the system responsibly. Users should not expect that files stored on servers or storage media are always private. During School, teachers will guide pupils towards appropriate materials. Outside of School, families bear responsibility for such guidance as they must also exercise with information sources such as television, telephones, movies, radio and other potentially offensive media.

10.5 Pupils must be polite and appreciate that other users might have different views than their own. The use of strong language, abusive language or aggressive behaviour is not allowed. Pupils must not write anything on a website or send by e-mail anything which could be offensive and/or defamatory of any person or organisation. They must not use the internet in or out of School to bully, threaten or abuse other pupils and they must not use the internet in or out of School for any purpose that may bring the School into disrepute. In addition, when using e-mail, pupils should also be aware:

10.5.1 E-mail should be written carefully and politely, particularly as messages may be forwarded or printed and be seen by unexpected readers.

10.5.2 Users are responsible for e-mail they send and for contacts made.

10.5.3 Anonymous messages and chain letters are not permitted.

10.6 Do:

10.6.1 Tell a member of staff if anything you come across on the internet offends you in any way.

10.6.2 Tell a member of staff if anything someone else is doing or looking at using a computer offends you in any way.

10.6.3 Use a secure password with a minimum of ten characters. This should be comprised of 2 or 3 random words, a number and a symbol. Try not to use anything that can be easily found out about yourself such as favourite colour or sports team. Do not write your password down or share it with anyone.

10.6.4 Check your School email account daily. Teachers use email to communicate with you.

10.6.5 Let ICT staff know if you are receiving lots of unwanted emails or if an email you are expecting does not arrive.

10.6.6 Inform the ICT support desk of any viruses.

10.6.7 Always log off when leaving the machine - your account is your responsibility. If the ICT department feel you are spending too long on the internet, your access will be withdrawn for a period of time (you will be warned by your tutor, if this is likely to happen).

10.6.8 Limit your internet time per day – you may be making good use of the internet but should not spend hours at one sitting in front of a computer screen; you are being monitored by the School, but you must monitor yourself too.

10.6.9 Be careful that you think about your own behaviour and about time management; talk to your tutor, your house staff or your Senior Tutor if you are worried about yourself or about someone else. It is easy to become addicted to time online, emailing or gaming.

10.6.10 Install anti-virus software on your machine(s) and keep it regularly updated.

10.6.11 Comply with the recommended specification for laptops, see the Laptop Advice for Parents document.

10.6.12 Keep regular back-ups of all work that you do on your laptop or other device, this is especially important if the work is assessed coursework.

10.7 Do not:

10.7.1 Store unnecessary files such as personal photos, animations, music files, or out of date coursework on the network. These files should be held on personal storage.

10.7.2 Give your password to anyone (including friends or teachers).

10.7.3 Allow anyone else to use your account. Remember that the account belongs to Roedean School and is for your use only. Your account remains active for the duration of your time at Roedean.

10.7.4 Disclose any personal information using ICT such as your age, your nationality, your mobile phone number, the School’s name, or any payment card details, such as a credit/debit card (if you have one). ICT includes email, chat rooms and texting unknown mobile phone numbers.

10.7.5 Eat or drink near a computer for obvious health and safety reasons.

10.7.6 Install or use any VPN, Proxy or any other software or system designed to keep your connection private

10.8 Further Guidance

10.8.1 Filtering software is used to filter out inappropriate sites and images but be aware that there is no perfect system for doing this.

10.8.2 ICT support staff can and may delete inappropriate files from your account, such as games, personal photographic or sound files if a problem arises.

10.8.3 Any information or file held or created on the Roenet system is the copyright of Roedean.

10.8.4 Your School account belongs to Roedean.

10.8.5 Information, documents, parts of documents, images on the web belong to someone else. You may be breaking copyright laws if you use or include them in your work.

10.8.6 Plagiarism is a serious offence. You should acknowledge by reference anything that you use in your work that you have taken from another source including web sites, emails, and textbooks (see the Roedean Behaviour Policy).

10.8.7 Internet access is switched off during the Summer Term 21:00 Y7, 21:30 Y8, 21:30 Y9, 22:00 Y10, 23:00 Y11 and Sixth Form access stops overnight at midnight.

11 Procedures

11.1 The way in which pupils relate to one another online can have a 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 spaces differ in many ways, the same standards of behaviour are expected online as apply offline. Use of technology and electronic devices should be safe, responsible, respectful to others and legal. If a pupil is aware of misuse by other pupils, she should talk to a teacher about it immediately.

11.1.1 An electronic device such as a mobile phone or a tablet computer may be confiscated in appropriate circumstances in accordance with the School's Good Behaviour [and Searching and Confiscation Policy.]

11.1.2 If there is good reason to suspect that the device has been, or could be used to cause harm, to disrupt teaching or break School rules, any data or files on the device may be searched and, where appropriate, data or files may be erased before the device is returned to its owner. Any search of an electronic device should be conducted in the presence of a member of the IT staff.

11.1.3 All electronic device checks and any searching and confiscation will be conducted in line with the school’s Promoting Good Behaviour Policy [and **Searching and Confiscation Policy**.]

11.2 Any misuse of technology by pupils will be dealt with under the School's promoting good behaviour policy and, where safeguarding concerns are raised, under the child protection and safeguarding policy and procedures.

11.3 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 preventing and tackling bullying policy. If a pupil thinks that they might have been bullied or that another person is being bullied, they should talk to a teacher or another trusted adult about it as soon as possible. See the School's preventing and tackling bullying policy for further information about cyberbullying and e-safety, including useful resources.

11.4 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 worse case scenarios, a culture that normalises abuse.

11.5 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 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 promoting good behaviour / child protection 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.

11.6 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 aware that this can occur online and / or face-to-face and can also occur simultaneously between the two.

11.7 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 be shared further (e.g. with the School's Designated Safeguarding Lead) to consider next steps. See Appendix 5 for further information.

11.8 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 child protection and safeguarding policy and procedures).

11.9 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, she must tell a teacher about it as soon as possible.

11.10 The School is also aware of the risk 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. Channel is a programme which focuses on support at an early stage to people who are identified as being vulnerable to being drawn into terrorism.

11.11 **Cybercrime**

11.11.1 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).

11.11.2 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, spyware, ransomware, botnets and Remote Access Trojans with the intent to commit further offence, including those above.

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

11.11.4 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.

11.12 In addition to following the procedures in the relevant policies as set out above, all serious incidents involving technology must be reported to the Designated Safeguarding Lead and the IT Manager who will record the matter centrally in the technology incidents log.

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 Proprietor has authorised the Head to apply any sanction which is appropriate and proportionate to the breach in accordance with the School's promoting good behaviour policy including, in the most serious cases, expulsion. Other sanctions might include: increased monitoring procedures withdrawal of the right to access the School's internet and email / electronic communication facilities; limited access to hardware]. 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 the School's promoting good behaviour policy (see Appendix 7 of the promoting good behaviour policy] for the School's policy on the searching and confiscation of electronic devices).

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 her parents for any costs incurred to the School as a result of a breach of this policy.

13 Passwords

13.1 Passwords protect the school systems from access by unauthorised people. Therefore, network passwords should never be given to anyone else without the IT Department's permission. Your password must meet these requirements:

13.1.1 The password should be least ten characters long.

13.1.2 The password must contain characters from at least three of the following four categories:

(a) Uppercase characters (A - Z)

(b) Lowercase characters (a - z)

(c) Base ten digits (0 - 9)

(d) Non-alphanumeric (For example: !, $, #, or %)

(e) The password cannot be the same as one of your last 24 passwords.

(f) The password should not be one you have used within 180 days.

(g) The password cannot contain your name or the school name.

(h) The password should be a secure passphrase using two to three random words.

14 Training

14.1 The School ensures that regular guidance and training is arranged on induction and at regular intervals thereafter so that all staff, including supply staff volunteers and Governors:

14.1.1 understand what is expected of them by this policy; and

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

14.1.3 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.

14.2 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-nude 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 as required at induction and at least annually thereafter.

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

14.4 The School maintains written records of all staff training.

15 Risk assessment

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

15.2 Furthermore, 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.

15.3 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.

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

15.5 Day to day responsibility to carry out risk assessments under this policy will be delegated to the Head of IT, who has been properly trained in, and tasked with, carrying out the particular assessment.

16 Record keeping

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

16.2 The records created in accordance 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 on its website privacy notices which explain how the School will use personal data.

17 Version control

Date of adoption of this policy	October 2022
Date of last review of this policy	October 2022
Date for next review of this policy	October 2023
Policy owner (SMT)	Director of Finance and Administration
Policy owner (Proprietor)	Council of Trustees

Appendix 1 Access and Security

1 Access to the internet from the School's computers and network must be for educational purposes only. You must not use the School's facilities or network for personal, social or non-educational use outside the permitted times specified by the School.

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 No laptop or other mobile electronic device may be connected to the School network without using Roedean log on details. The IT manager may refuse access to the network for any device that does not adhere to our security requirements, or that pose a threat to the network. All electronic devices that are to be connected to the School network must have installed appropriate Anti-Virus protection, which is kept up to date, a Firewall enabled and secured with a reasonable strong password.

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 is strongly discouraged, as pupils are unable to benefit from the School's filtering and anti-virus software. Pupils should not use cellular data at all in lessons, whether on their tablets, or by hot spotting with mobile phones. 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.

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 Head of IT.

7 You must not attempt to access or share information about others without the permission of a member of staff. 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 Head 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 attempt to disable, defeat or circumvent any of the School's filtering systems. 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 / electronic communications. If you think or suspect that an attachment, or other downloadable material, might contain a virus, you must speak to Head of IT 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 strongly 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 use the School's computer system for educational purposes only and are not permitted to access interactive or networking websites outside the permitted times specified by the School.

3 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.

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 ICT Manager.

5 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.

6 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.

7 You must not install or use any VPN, proxy or other software designed to keep your connection private.

8 You must not communicate with staff using social networking sites or other internet or web-based communication channels unless this is expressly permitted for educational reasons.

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

Use of email / electronic communication services

10 You must not use any personal web-based email accounts such as Gmail, Yahoo or Hotmail or electronic communication devices, apps or platforms through the School's network outside the permitted times specified by the School. This will be unnecessary as you are provided with your own personal email account for School purposes.

11 Your School email / electronic communication accounts can be accessed from home by visiting webmail.roedean.co.uk (email) or the pupil portal. The School will not forward messages received during the School holidays.

12 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 account or to a member of staff's personal account is not permitted.

13 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 Head and / or your parents would consider to be inappropriate. Remember that messages could be forwarded to or seen by someone you did not intend.

14 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 messaging system in this way is a serious breach of discipline and may constitute a criminal offence.

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

16 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 promoting good behaviour policy and also as a safeguarding matter under the School's child protection and safeguarding policy and procedures.

17 Online bullying is considered as serious as any other form of bullying and will be dealt with in accordance with the School's preventing and tackling bullying policy.

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

19 You must not read anyone else's messages without their consent.

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, MP3 players and wearable technology.

2 All mobile electronic devices brought onto School premises must be made known to the pupil's Head of Year.

3 Students in Years 7 to 10 will be asked to hand their mobile phone in to their Head of Year when they arrive in the morning. It will be stored securely and available to collect at the end of the school day.

4 For students in Years 11, 12 and 13, Mobile phones and other mobile electronic devices must be switched off (and not just on silent mode) and kept in bags during School hours, including at break times and between lessons. In certain circumstances, a pupil may be given permission to use their own mobile device or other smart technology to connect to the internet using the School's network. Express permission to do so must be sought and given from a member of staff in advance.

5 The School does all that it 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 text 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..

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 system protections. 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.

7 The use of mobile phones during the School day will not be necessary. 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 office and a message will be relayed promptly.

8 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 with the Deputy Head: Academic or the SENCO in writing.

9 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.

10 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 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 preventing and tackling bullying policy and promoting good behaviour policy]) and the School's safeguarding procedures will be followed in appropriate circumstances (see the School's child protection and safeguarding policy and procedures).

11 Pupils must not use their mobile and smart technology to send abusive, 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 promoting good behaviour policy and also as a safeguarding matter under the School's child protection and safeguarding policy and procedures. Please see the ‘Promoting Good Behaviour’ policy for full details.

12 Mobile electronic devices may be confiscated and searched in appropriate circumstances. Please see Sections 7.3 and 7.4 of the School's promoting good behaviour policy] on the searching of electronic devices. You may also be prevented from bringing a mobile electronic device into the School temporarily or permanently and at the sole discretion of the Head.

13 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 12.3 of this policy.

3 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.

4 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 a child.

5 The posting of images which in the reasonable opinion of the Head is considered to be offensive or which brings the School into disrepute 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.

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

6.1 "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.

6.2 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.

6.3 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 doing certain jobs in the future.

6.4 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.

6.5 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.

6.6 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.

6.7 Even if you do not 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.

6.8 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 child protection and safeguarding policy and procedures).

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

6.10 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.

7 Upskirting

7.1 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.

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

7.3 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.

7.4 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 child protection and safeguarding policy and procedures).

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

Appendix 5 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 promoting good behaviour policy and also as a safeguarding matter under the School's child protection procedures (see the School's child protection and safeguarding 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;

5.2 sexualised online bullying;

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

5.4 sexual exploitation, coercion or threats; and

5.5 coercing others into sharing images of themselves or performing acts they are 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 child protection and safeguarding 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 promoting good behaviour policy.

Appendix 6 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 child protection and safeguarding 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 promoting good behaviour policy].

6 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 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 school promoting good behaviour policy.

Appendix 7 Pupil Code of Conduct: Online Learning

Keeping Everyone Safe

While learning online and remotely, both during timetabled hours and during school-related activities, you are expected to follow these basic rules, procedures, and expectations:

Your first priority at school, and therefore with online education is to learn. Avoid distractions that interfere with or undermine that key purpose. Keep your phone and personal emails turned off, as you would if you were in school.

Be ready with appropriate materials, with all required preparation work, properly dressed, and ready to work at the designated time that the class begins.

Only use school-designated and agreed forums for communication, which in this case are limited to Microsoft Teams, SharePoint, and School Email only.

Use school-appropriate language and behaviour at all times, while maintaining friendly and courteous behaviour.

Be polite and respectful to everyone, including other students, teachers, support staff, and your parents/guardians. Follow individual teacher instructions, class rules, and expectations at all times.

Continue to follow our IT Acceptable Use Policy for Students that you signed at the start of the year.

Do not set up your own Teams or Channels or use the Chat function in Microsoft Teams.

Use online materials, recordings, and access respectfully, by agreeing never to record, take screenshots or photos, or share materials involving a pupil or teacher.

Online attendance and participation in class are an essential part of your education, and attendance online is the responsibility of both you and your parents.

Provide feedback so we can improve things for you.

Make sure your online environment is suitable and safe by working in an appropriate space in your home, and with an adult around for help and support.

Please contact your Head of Year if you have any concerns but avoid sharing your anxieties with your friends if we can help solve them for you.

If you have any technical issues, please contact the IT helpdesk: helpdesk@roedean.co.uk

Read, understand, and sign our key safeguarding permissions wufoo to protect yourself and others.

You will need to complete the wufoo form below to enable you to take part in live online learning. Please do this now. Thank you.

https://roedean.wufoo.com/forms/pupils-consents-for-remote-learning/

Please keep this and the information poster below to help to keep you safe and so that you are clear how to work well remotely.

Appendix 8 Parent Code of Conduct for Remote Learning

Keeping Everyone Safe

While learning online and remotely, both during timetabled hours and during school-related activities, your daughter is expected to follow these basic rules, procedures, and expectations:

Her first priority at school, and therefore with online education, should be to learn. Please help her to avoid distractions that interfere with or undermine that key purpose, eg. to keep her phone and personal emails turned off during the school day.

Please help her to have the appropriate materials, with all required preparation work, and be ready to work at the designated time that class begins. She should be properly and appropriately dressed, so bed wear is not suitable.

Your daughter is only permitted to use school-designated and agreed forums for communication, which in this case are limited to Microsoft Teams, SharePoint, and School Email only.

Pupils are not allowed to set up your own Teams or Channels or use the Chat function in Microsoft Teams – please can you check that the only Teams your daughter belongs to have been set up by a teacher.

Please encourage her to use school-appropriate language and behaviour at all times, while maintaining friendly and courteous behaviour. Informal language is normal outside of school, so she may need a reminder to avoid using emoji's or 'xx', for example, when she is communicating in Microsoft Teams.

Please be aware that she has been reminded to be polite and respectful to everyone, including other students, teachers, support staff, and you.

Please read the attached IT Acceptable Use policy that your daughter signed at the start of the year. Please ensure she is reminded to adhere to this.

It is important to ensure that she never records, takes screenshots or photos, or shares materials involving a pupil or teacher.

Online attendance and participation in class are an essential part of her education and attendance online, as for school, is your and our responsibility. We will contact you if your daughter is not 'attending lessons' as required.

Please make sure her online environment is suitable and safe by encouraging her to work in an appropriate space in your home, being available if she needs help and support.

Please contact the school as indicated below if you have any concerns, and do not share concerns on social media in order to avoid spreading undue anxiety.

Your daughter's Head of Year for any concerns or feedback.

The IT helpdesk if you have any technical issues: helpdesk@roedean.co.uk

Please keep this and the information poster below to help to keep you safe and clear how to work well remotely.

Appendix 9 Pupil and Parent Personal Electronic Devices Agreements

Pupil Personal Electronic Devices Agreement

I, __________________, understand that bringing a personal electronic device to school is a privilege that may be taken away if I abuse it. I agree to abide by the policy and understand the consequences if I fail to do so.

Signed by

Pupil	**Date**
Parent	**Date**
Form tutor	**Date**

Parental Personal Electronic Devices Agreement

I, __________________, recognise that **Roedean School** bears no responsibility for personal electronic devices lost, damaged or stolen on school property or on journeys to and from school. I agree to the terms of this policy and will discuss the responsibility of owning a personal electronic device with my child (name) __________________. I understand that a teacher may confiscate devices used in an unacceptable manner as detailed in the policy.

Signed by

Parent	**Date**
Form tutor	**Date**

Appendix 10 Personal Electronic Devices FAQs

Frequently Asked Questions (FAQ'S)

Q: Can anyone bring in a laptop or tablet?

A: Currently pupils in years 10-13 are able to bring in tablets and laptops, but that might change in the future, so keep an eye on bulletins and information from your Head of Year.

Q: What personal ICT Devices can we use in School?

A: You can use either a laptop, tablet device, chrome-book or any other compatible device that supports the 802.1x wireless standard. All devices should allow you to type so tablets should have a separate Bluetooth keyboard.

If you need to run any specialist academic software to help with your studies, you will be advised of any required computer hardware and software specifications separately by your subject teachers.

Q: What personal ICT Devices are not allowed in School?

A: You cannot bring in your own desktop computer for use in school.

Q: Can we physically plug in our devices to the School Network using a network data cable?

A: Unfortunately, not, access to the network can only be permitted via the wireless network.

Q: Do we need permission to use a personal device in School?

A: Both you and your parents have been asked to read and agree to the terms and conditions set out in the ICT Acceptable Use Policy. Once you have done that, then you are able to use a personal device as outlined in your year group's guidelines.

Q: Once consents have been completed, how can we access the wireless network on our personal devices?

A: You should connect your device(s) to the network by using your normal School username and password (the same as for your school email). You should follow instructions from your IT induction to get connected. It is important to connect via the school's network to gain access to useful software, and to keep you safe online.

Q: Does the School provide any ICT technical support for any issues that arise with our personal devices?

A: You should be familiar with how to use your device and your teachers will incorporate the use of devices into learning where relevant. The IT technicians are able to provide technical support if you have a technical issue.

Q: Do I have to buy something now?

A: No. You can bring in a device anytime up until the time you leave the School. There is no time-limit on when you might want to log into the network.

Q: Are pupil personal devices insured under the School's insurance policy?

A: You accept full responsibility for your device, and you should keep it with you or locked away at all times. Whilst the School provides secure lockable lockers, the school is not responsible for the security (including loss, damage or theft) of any device that is not defined as the property of the School. School insurance cover will therefore not be applicable or valid.

The school would therefore encourage you to ask your parents to extend their home insurance policy under the personal possessions section or, alternatively, cover electronic devices by a separate policy.

If a device is stolen or damaged, the school will investigate. Any incidents should be reported to your head of year straight away and these will be logged.

Q: How can we charge our devices at school?

A: Your devices should be charged at home or in the boarding houses, wherever possible. All electrical devices used in school need to be Portable Appliance Tested (PAT) so, for Health and Safety reasons, personal devices cannot be charged in School unless they have undergone this testing. The Director of Sixth Form will organise PAT testing days to manage this for sixth form students.

Q: Can we use our own personal ICT devices in class?

A: Devices may only be used in class with the approval of the class teacher. Sixth form students may use devices in class if this is their preference.

Q: Can we use our device as a personal Wi-Fi Hotspot or broadcast our own wireless network to allow others to access the internet?

A: You are not permitted to use your device as a ‘Hotspot’ so that it can allow others to access the internet by by-passing the School’s wireless network whilst in School.

Any pupil enabling such a network would be committing a breach of trust that could result in them no longer being able to use a personal ICT device in School. Additional sanctions could also apply, depending on the consequences of accessing mobile data in this way.

Q: Why are we filtered and monitored on our own devices? Shouldn’t we be able to see what we want to on our own device?

A: The School is providing pupils with a service, whilst being committed to making sure the network is safe and secure as possible. This is also part of our wider duty of care. Any personal device using the School’s wireless network is filtered, monitored and secured according to policy. Our wireless network is there to help support teaching and learning, and not as a recreational tool, during the school day. Boarders will be able to access recreational sites in the evenings and on weekends.

The School cannot be responsible for any content accessed by a user using their own devices through non-School controlled wireless systems such as personal 3G, 4G and 5G networks, ‘Hotspots’, Proxy or VPN bypass Systems.

Q: What if we cannot bring in a laptop or device?

A: The School has many rooms and areas where you can access computers before, during and after the School day. Additionally, if access to devices is required for a particular lesson, teachers will book School devices. Quality learning can also take place without the need for technology. Traditional approaches to learning are still appropriate and, importantly, work, so do not worry.

Q: Can we access any School specific teaching and learning software including our school network data files from our personal device?

A: You can access a range of School Document files from your personal computer devices via the School’s intranet, SharePoint and Teams accounts

You can also now login with your normal School network username and password and use Office 365 online – accessible via the school website.

Office 365 offers the following benefits:

- Accessible from any computer with an Internet connection and also works across a range of mobile devices.
- Ability to create and store up to 5TB of data files into your OneDrive Data area using the Microsoft online apps for Word, Excel, PowerPoint and OneNote (no software installation necessary).