ROEDEAN

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

Policy Area	Safeguarding
Author	IT Manager
Relevant Statutory Regulations	Education (Independent School Standards) Regulations, April 2026 National Minimum Standards for Boarding Schools (DfE, May 2026) 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 2026)
Senior Team Lead	Director of Strategy and Innovation
Version	2026.1
Last Updated	August 2026
Review Date	**August 2027**

Contents

1 Overview ... 3
2 Aims ... 3
3 Scope and application ... 3
4 Regulatory framework ... 4
5 Definitions ... 5
6 Filtering & Monitoring ... 6
7 Password Policy ... 7
8 Security and Protecting Information ... 8
9 Using Technology in School ... 8
10 Internet & Electronic Communications ... 9
11 School-owned Devices ... 10
12 Personal Devices ... 10
13 Social Media ... 11
14 Reporting Misuse ... 11
15 School Rules ... 11
16 Helpful Resources ... 12
17 Further information ... 12
18 Procedures ... 13
19 Cybercrime ... 14
20 Sanctions ... 14
Appendix 1 Access and Security ... 15
Appendix 2 Use of the internet and email / electronic communication services ... 16
Appendix 3 Use of mobile electronic devices and smart technology ... 18
Appendix 4 Photographs and images ... 20
Appendix 5 Online sexual harassment ... 22
Appendix 6 Harmful online challenges and online hoaxes ... 23
Appendix 7 Pupil Code of Conduct: Online Learning ... 24
Appendix 8 Parent Code of Conduct for Remote Learning ... 25

1 Overview

1.1 At Roedean School, we believe that technology is an essential part of your learning experience. To ensure a safe and productive environment, we have established guidelines for using technology, including the internet, laptops, and other devices. Please read this agreement carefully with your parent or guardian. You will be asked to accept this policy on your first use of a computer and refreshed at the start of each term.

2 Aims

2.1 This is the acceptable use policy for pupils of Roedean School (School).

2.2 The aims of this policy are as follows:

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

2.2.2 to safeguard and promote your welfare, 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.

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

2.2.4 to help you take responsibility for your own safe use of technology;

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

2.2.6 to prevent the unnecessary criminalisation of pupils; and

2.2.7 to help to promote a whole school culture of openness, safety, equality and protection.

2.3 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.

3 Scope and application

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

3.2 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.

3.3 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:

3.3.1 The voice and data networks that connect them.

3.3.2 All devices connected to these computers and networks.

3.3.3 The hardware and software associated with these systems.

3.3.4 The information managed by these systems.

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

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

4 Regulatory framework

4.1 This policy has been prepared to meet the School's responsibilities under:

4.1.1 Education (Independent School Standards) Regulations, April 2026;

4.1.2 National Minimum Standards for Boarding Schools (DfE, May 2026);

4.1.3 Education and Skills Act 2008;

4.1.4 Children Act 1989;

4.1.5 Data Protection Act 2018 and UK General Data Protection Regulation (UK GDPR); and

4.1.6 Equality Act 2010.

4.2 This policy has regard to the following guidance and advice:

4.2.1 Keeping children safe in education (DfE 2026) (KCSIE);

4.2.2 Preventing and tackling bullying (DfE, 2017);

4.2.3 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), 2020 updated March 2024);

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

4.2.5 Searching, screening and confiscation: advice for schools (DfE, 2023);

4.2.6 Behaviour in schools: advice for headteachers and school staff (DfE, 2024)

4.2.7 Relationships education, relationships and sex education and health education guidance (DfE, 2025).

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

4.3.1 Promoting Good Behaviour Policy;

4.3.2 Preventing and tackling Bullying Policy;

4.3.3 Online Safety Policy;

4.3.4 Exclusions Policy

4.3.5 Safeguarding and Child Protection Policy and Procedures;

4.3.6 Risk Assessment Policy for Pupil Welfare; and

4.3.7 RSE Policy (Relationships and Sex Education).

5 Definitions

5.1 Before you proceed, familiarise yourself with these key terms:

5.1.1 **Technology**: Includes all ICT systems at the school, encompassing the internet.

5.1.2 **School-owned devices**: Devices provided by the school for educational purposes, such as laptops and tablets.

5.1.3 **Personal devices**: Devices owned by students, brought into school, including mobile phones.

5.1.4 **Staff**: 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.

5.1.5 **Sexual Harassment**: Unwanted conduct of a sexual nature

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 Interactive 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 Filtering & Monitoring

6.1 The school utilises a robust filtering and monitoring system to protect students from harmful content and to identify safeguarding issues. The use of any device connected to the School's network will be logged and monitored by the IT Department and Safeguarding team.

6.2 The school's filtering and monitoring systems are in place to prevent access to harmful online content and to proactively identify safeguarding risks, whether on or off school premises. By using a school-managed device, students consent to this comprehensive monitoring of all activity.

6.3 The school's approach to filtering and monitoring is reviewed at least annually to ensure we meet the DfE's Filtering and Monitoring Standards and effectively block illegal and inappropriate content without unreasonably impacting education.

6.4 The **Designated Safeguarding Lead (DSL)** holds the lead responsibility for the strategic oversight, effectiveness, and regular review of the school's online safety, filtering, and monitoring systems and processes.

6.5 For the protection of all pupils, pupil use of email / electronic communication and use of the internet will be monitored by the School. You should remember that even when an email / electronic message or anything that has been downloaded has been deleted, it can still be traced.

6.6 To ensure student e-safety and welfare, the school implements a screen monitoring system. This monitoring is installed on school-owned student devices and devices from the 1:1 scheme. Monitoring occurs whether the device is on or off school premises. The system actively captures and analyses all on-screen activity, including typed and deleted text, search queries, emails, web chats, social media, and documents, with the primary purpose of preventing and detecting illegal, harmful, or unacceptable activity related to safeguarding risks. The system is configured to detect activity across the following categories:

6.6.1 Mental Health issues

6.6.2 Self-Harm and Suicide

6.6.3 Bullying

6.6.4 Violence and Aggressive behaviour

6.6.5 Radicalisation and Extremism

6.6.6 Sexual Exploitation and Grooming

6.6.7 Sharing of harmful images

6.6.8 Oversharing personal information

6.6.9 Substance abuse (including alcohol and drugs)

6.7 All critical alerts generated by the monitoring system are immediately reviewed by a contracted, specialised safeguarding monitoring team. Upon verification, these alerts are escalated to the school's Designated Safeguarding Lead (DSL) and the wider safeguarding team. All reported incidents will be thoroughly investigated in line with the school's safeguarding and disciplinary procedures. Inappropriate or harmful use will result in disciplinary action and, where a legal or child protection risk is identified, referral to external agencies such as the police or social services. All data (e.g., screenshots, logs) retained as part of a confirmed incident will be securely erased after 15 months.

6.8 You should not assume that any files stored on Roedean's network or cloud services are private.

6.9 The School uses several systems such as Filtering, Anti-Virus, Anti-Malware and Firewalls to protect and monitor internet access.

6.10 Staff may review files and communications to ensure that users are using the system responsibly.

6.11 During School, teachers will guide you 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.

6.12 If a member of staff feels like a you are spending too much time on the internet, access will be withdrawn for a period of time. (You will be warned by your tutor or Head of Year if this is likely to happen).

6.13 You must not create, share, or access content that is illegal, malicious, or that constitutes misinformation, disinformation, or conspiracy theories. This includes any content that has the potential to cause harm, offense, or distress to others.

6.14 The school uses AI tools with appropriate filtering and monitoring. Students are expected to use AI responsibly and should consult our Artificial Intelligence Usage Policy for full details and rules.

6.15 All policies including ones relating to Plagiarism apply to work produced with the help of AI.

7 Password Policy

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

7.1.1 The password should be least 12 characters long.

7.1.2 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) Number (0 - 9)

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

7.1.3 The password cannot be the same as one of your last 24 passwords.

7.1.4 The password should not be one you have used within 180 days.

7.1.5 The password cannot contain your name or the school's name.

7.1.6 The password cannot use a word from a banned common passwords list such as "password", "brighton" etc.

7.1.7 The password should be a secure passphrase using two to three random words.

8 Security and Protecting Information

8.1 I will:

8.1.1 Make sure I understand how to keep my information safe when using technology; consult my teacher if I have questions.

8.1.2 Inform the IT Department of any suspected viruses.

8.1.3 Always log off when leaving a computer. Your account is your responsibility.

8.1.4 Install an Anti-Virus package on my devices and ensure it is regularly updated.

8.1.5 Keep regular backups of all work. – Speak to the IT Department for advice if needed.

8.2 I will not:

8.2.1 Attempt to bypass any security measures implemented by the school on the internet or school-owned devices.

8.2.2 Share passwords with others. My account is uniquely for my own use.

8.2.3 Allow anyone else to use my account. Remember: The account belongs to Roedean School and is for your use only.

9 Using Technology in School

9.1 I will:

9.1.1 Only use technology and devices with permission.

9.1.2 Access only approved websites, apps, and online platforms.

9.1.3 Utilise school ICT facilities for schoolwork.

9.1.4 Limit non-school related internet usage to break/lunch times and after school.

9.1.5 Safeguard USB sticks and removable media containing schoolwork.

9.2 I will not:

9.2.1 Install software on school ICT systems without authorization from the IT Department.

9.2.2 Search for, view, download, upload, or send inappropriate content on the internet.

9.2.3 Store unnecessary files such as personal photos, animations, music or videos on the Schools' systems. These files must be held on personal storage.

10 Internet & Electronic Communications

10.1 I will:

10.1.1 Use the school-provided email account for school-related communication only.

10.1.2 Seek advice from a member of staff if I am unsure I am doing the right thing.

10.1.3 Only use my school username and password to connect any personal device to the network unless I have permission from the IT Department.

10.1.4 Be polite and appreciate that other users might have different views than my own.

10.1.5 Write e-mail and communications carefully and politely, particularly as messages may be seen by unexpected readers.

10.1.6 Tell a member of staff if anything I come across on the internet offends me in any way.

10.1.7 Tell a member of staff if anything someone else is doing or looking at offends me in any way.

10.1.8 Check my School email account daily.

10.1.9 Let the IT Department know if I am receiving lots of unwanted emails or if an email I am expecting does not arrive.

10.1.10 Limit my time on the internet/device. You may be making good use of the internet but should not spend hours at one time sitting in front of a computer screen; talk to your tutor, your house staff or your Head of Year if you are worried about yourself or about someone else. It is easy to become addicted to time online, emailing or gaming.

10.1.11 Attribute and reference any work created or contributed to by AI tools. Unattributed submission of AI-generated content may be treated as plagiarism or academic misconduct.

10.2 I will not:

10.2.1 Open emails from unknown senders.

10.2.2 Use personal email for schoolwork without staff permission.

10.2.3 Provide my username and password to others.

10.2.4 Provide personal information to anyone on the internet or by e-mail, such as my age, nationality, mobile number, the School's name or payment card details.

10.2.5 Send anonymous messages and chain letters.

10.2.6 Share any material which may infringe copyright, intellectual property or is likely to be unsuitable for children of 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 I am unsure, I must ask a teacher.

10.2.7 Use strong language, abusive language or aggressive behaviour.

10.2.8 Not write anything on a website or send by e-mail anything which could be offensive and/or defamatory of any person or organisation.

10.2.9 Use the internet in or out of School to bully, threaten or abuse other pupils.

10.2.10 Use the internet in or out of School for any purpose that may bring the School into disrepute.

10.2.11 Install or use any VPN, Proxy or any other software/technology designed to keep private connections.

10.2.12 Enter personally identifiable or sensitive school/student information into a public-facing AI Tool.

10.2.13 Use AI to generate or distribute content that violates this AUP.

10.2.14 Seek out, create, or distribute content that promotes or constitutes safeguarding harms, including **misinformation, disinformation (fake news), or conspiracy theories**, as these can lead to radicalisation, harassment, and other serious safeguarding issues.

11 School-owned Devices

11.1 I will:

11.1.1 Use school-owned devices exclusively for schoolwork.

11.1.2 Access only approved websites and apps.

11.1.3 Acknowledge that device usage is monitored.

11.1.4 Care for school-owned devices.

11.1.5 Report damage, loss, or security concerns promptly.

11.1.6 Replaced lost or damaged equipment.

11.2 I will not:

11.2.1 Use school-owned devices for inappropriate content or personal social media.

11.2.2 Eat or drink near a computer.

12 Personal Devices

12.1 I will:

12.1.1 Use personal devices only during break and lunch times unless otherwise agreed with a member of staff.

12.1.2 Ensure devices are switched off during lessons and kept securely.

12.1.3 Acknowledge that the school is not responsible for costs if personal devices are lost, damaged, or stolen.

12.1.4 Hand my mobile phone into my Head of year on arrival into school if I am in Year 7 – 10 and collect it upon my departure/at the end of the day.

12.2 I will not:

12.2.1 Use personal devices for inappropriate content or personal social media.

12.2.2 Use my mobile in communal settings nor have it visible in the dining room, co-curricular activities, assemblies and house meetings unless express permission is given by a member of staff.

12.3

12.3.1 Content viewed and opened on a school device, including when off-site, must follow school guidelines and non-appropriate content, such as but not limited to, gambling, pornography or illegal content must not be accessed.

12.3.2 Signing into a browser or other software that synchronises data on both a personal and school device (e.g. Microsoft Edge) may pull through data from your personal device onto a school device and will therefore be subject to the school's monitoring systems.

13 Social Media

13.1 I will:

13.1.1 Be mindful of posting content about the school.

13.2 I will not:

13.2.1 Engage with school staff on social media.

13.2.2 Accept or send friend or follow requests to school staff.

13.2.3 Send inappropriate messages or engage in bullying through social media.

14 Reporting Misuse

14.1 I will:

14.1.1 Recognise that internet usage is monitored.

14.1.2 Understand that disciplinary action may be taken, following the Promoting Good Behaviour Policy, if this agreement is violated.

15 School Rules

15.1 You **must** be aware of and observe rules and principles:

15.1.1 All students are expected to adhere to the highest standards of behaviour online. Online behaviours that constitute bullying, sexual violence, sexual harassment, or the distribution of explicit imagery (including child-on-child abuse) will be treated with the **same seriousness** as offline abuse and will result in serious disciplinary action and/or referral to external agencies.

15.1.2 All students have a personal responsibility to report any content or activity—whether seen on a school device or on a private device outside of school—that causes concern or

violates this policy, to a member of staff or the Designated Safeguarding Lead (DSL) immediately.

15.1.3 Access and Security rules as set out in Appendix 1;

15.1.4 Use of the internet and email / electronic communication services as set out in Appendix 2;

15.1.5 Use of mobile electronic devices and smart technology as set out in Appendix 3;

15.1.6 Photographs and images (including the consensual and non-consensual making or sharing of nude and semi-nude images and videos) as set out in Appendix 4;

15.1.7 Online Sexual Harassment as set out in Appendix 5; and

15.1.8 Harmful online hoaxes and challenges as set out in Appendix 6.

16 Helpful Resources

16.1 You may find the following resources helpful in keeping yourself safe online:

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

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

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

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

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

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

16.1.7 https://shorespace.org.uk/

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

17 Further information

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

17.2 IT Staff can and may delete inappropriate files from your account.

17.3 Any information or file held or created on the School's systems is the copyright of Roedean School.

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

17.5 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 websites, emails, artificial intelligence (generative AI) and textbooks (see the Promoting Good Behaviour Policy and Artificial Intelligence Usage Policy).

17.6 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.

18 Procedures

18.1 An electronic device such as a mobile phone or a tablet computer may be confiscated in appropriate circumstances in accordance with the Promoting Good Behaviour Policy. (See Searching and Confiscation Policy).

18.2 If there is good reason to suspect that the device has been, or could be used to cause harm, to disrupt teaching or to 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 Department.

18.3 All electronic device checks and any searching and confiscation will be conducted in line with the Promoting Good Behaviour Policy and Searching and Confiscation Policy.

18.4 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 Safeguarding and Child Protection Policy and Procedures.

18.5 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 you think that you might have been bullied, or that another person is being bullied, you should talk to a teacher or another trusted adult about it as soon as possible. See the Preventing and tackling Bullying Policy for further information about cyberbullying and e-safety, including useful resources.

18.6 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.

18.7 You must not use your 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 / Safeguarding Policies. If you think that you might have been sexually harassed or that another person is being sexually harassed, you should talk to a teacher about it as soon as possible.

18.8 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. You 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.

18.9 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 Safeguarding and Child Protection Policy and Procedures.

18.10 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.

19 Cybercrime

19.1 Cybercrime is a criminal activity committed using computers and / or internet. Cybercrimes include, but not limited to:

19.1.1 Unauthorised access to a computer (illegal 'hacking'), for example, accessing a school's computer network to look for a test paper answers.

19.1.2 Denial of service (DoS or DDoS) attacks, which are attempts to make a computer, network or website unavailable by overwhelming it.

19.1.3 Making, supplying or obtaining malicious software such as viruses, spyware, ransomware, botnets and trojans with the intent to commit further offence.

19.2 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.

20 Sanctions

20.1 Where a pupil breaches any of the School's rules, practices or procedures set out in this policy or the appendices, sanctions appropriate and proportionate to the breach with be applied in accordance with the School's Promoting Good Behaviour Policy.

20.2 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.

20.3 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.

20.4 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.

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 IT Department.

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 IT Department.

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 IT Manager 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 IT 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. This is in line with the Artificial Intelligence Policy.

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 misinformation, disinformation, conspiracy theories, 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 Safeguarding and Child Protection 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 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 or wearable technology 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 or if you require a PEEP. 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 Safeguarding and Child Protection 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 Safeguarding and Child Protection 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 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 20.3 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 20.3 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 **Making or sharing nude and semi-nude images and videos**

6.1 "Making or sharing nudes and semi-nudes" means the consensual and non-consensual creation, sending or posting of nude or semi-nude images, videos or live streams by young people under the age of 18 online, including where such images have been digitally altered or generated using artificial intelligence (sometimes referred to as "deepfakes" or "deep nudes"). 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.

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 Safeguarding and Child Protection 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 Safeguarding and Child Protection 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 making or 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 Designated Safeguarding Lead (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 Professionals 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 ICT Acceptable Use Policy for Pupils.

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: it@roedean.co.uk

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

You will need to complete the electronic form to enable you to take part in live online learning.

Please keep this information 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, e.g. 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 ICT Acceptable Use Policy for Pupils. 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: it@roedean.co.uk

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