ROEDEAN

POLICY TITLE	**Online Safety Policy**

Policy Area	Safeguarding
Author	Deputy Head: Pastoral
Relevant Statutory Regulations	The Education (Independent School Standards) Regulations 2014; Boarding schools: national minimum standards (Department for Education (DfE), April 2022); Education and Skills Act 2008; Children Act 1989; Data Protection Act 2018 and UK General Data Protection Regulation (UK GDPR); and Equality Act 2010. Keeping Children Safe in Education (KCSIE 2025) Mobile Phones in Schools (DfE), February 2024 DfE Guidance on Generative AI in Education (DfE, 2025)
Senior Team Lead	Deputy Head: Pastoral
Version	2025.2
Last Updated	August 2025
Review Date	**August 2026**

Contents

1 Aims

1.1 This is the online safety policy of Roedean School (**School**).

1.2 At Roedean School we understand that technology is an essential resource for supporting teaching and learning. The internet, and other digital and information technologies, open up opportunities for pupils and play an important role in their everyday lives.

1.3 Whilst the School recognises the importance of promoting the use of technology throughout the curriculum, we also understand the need for safe internet access and appropriate use. This is particularly important during extended periods of online learning due to Covid-19.

1.4 The aim of this policy is to promote and safeguard the welfare of all pupils through the implementation of an effective online safety strategy which:

1.4.1 protects the whole School community from illegal, inappropriate and harmful content or contact;

1.4.2 educates the whole School community about their access to and use of technology;

1.4.3 establishes effective mechanisms to identify, intervene and escalate incidents where appropriate; and

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

1.4.5 monitors online use and filters appropriately; regularly reviewing the effectiveness of any systems employed to this end

1.5 This policy forms part of the School’s whole school approach to promoting child safeguarding and wellbeing, which seeks to ensure that the best interests of pupils underpins and is at the heart of all decisions, systems, processes and policies.

1.6 Online safety is a running and interrelated theme throughout many of the School's policies and procedures (including its child protection and safeguarding policy and procedures]) and careful consideration has been given to ensure that it is also reflected in the School's curriculum, teacher training and any parental engagement, as well as the role and responsibility of the School's Designated Safeguarding Lead.

1.7 The School is committed to providing a safe learning and teaching environment for all pupils and staff, and has implemented important controls to mitigate the risk of harm.

2 Scope and application

2.1 This policy applies to the whole School.

2.2 This policy applies to all members of the School community, including staff and volunteers, pupils, parents and visitors, who have access to the School's technology whether on or off School premises, or otherwise use technology in a way which affects the welfare of other pupils or any member of the School community or where the culture or reputation of the School is put at risk.

3 Regulatory framework

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

3.1.1 The Education (Independent School Standards) Regulations 2014;

3.1.2 Boarding schools: national minimum standards (Department for Education (**DfE**), April 2015);

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.

This policy has regard to the following guidance and advice:

3.1.7 Keeping children safe in education (DfE, September 2025) (**KCSIE**) including safeguarding consideration related to emerging technologies such as generative Artificial Intelligence (AI);

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

3.1.9 Sharing nudes and semi-nudes: advice for education settings working with children and young people (UKCIS, March 2024);

3.1.10 Revised Prevent duty guidance: for England and Wales (DfE 2023 updated 2024);

3.1.11 Channel duty guidance: protecting vulnerable people from being drawn into terrorism (Home Office, February 2023);

3.1.12 Searching, screening and confiscation: advice for schools (DfE, July 2022);

3.1.13 Relationships Education, Relationships and Sex Education (**RSE**) and Health Education guidance (DfE, September 2021);

3.1.14 Teaching online safety in schools (DfE, January 2023);

3.1.15 Harmful online challenges and online hoaxes (DfE, February 2021);

3.1.16 Online safety guidance if you own or manage an online platform (DfDCMS, June 2021);

3.1.17 A business guide for protecting children on your online platform (DfDCMS, June 2021);

3.1.18 Online safety audit tool (UKCIS, October 2022); and

3.1.19 Mobile Phones in Schools (DfE, February 2024).

3.1.20 DfE Guidance on Generative AI in Education (DfE, 2025)

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

3.2.1 ICT acceptable use policy for pupils;

3.2.2 preventing and tackling bullying policy

3.2.3 safeguarding and child protection policy and procedure

3.2.4 data breach policy and procedure

3.2.5 camera use policy

3.2.6 ICT acceptable use policy: staff;

3.2.7 code of conduct for staff policy;

3.2.8 risk assessment policy for pupil welfare;

3.2.9 whistleblowing policy;

3.2.10 data protection and ICT acceptable use policy;

3.2.11 school rules and

3.2.12 RSE policy (relationships and sex education)

4 Publication and availability

4.1 This policy is available in hard copy on request.

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

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

5 Definitions

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

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

5.3 In considering the scope of the School's online safety strategy, the School will take a wide and purposive approach to considering what falls within the meaning of technology, networks and devices used for viewing or exchanging information (collectively referred to in this policy as **technology**).

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 The Proprietor is required to ensure that all those with leadership and management responsibilities at the School actively promote the well-being of pupils. The adoption of this policy is part of the Proprietor's response to this duty.

6.3 To ensure the efficient discharge of its responsibilities under this policy, the 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	Deputy Head: Pastoral	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	IT Manager	As required, and at least termly

visited), relevant risk assessments and any action taken in response and evaluating effectiveness		
Online safety	Director of Safeguarding and Deputy Head: Pastoral	
Seeking input from interested groups (such as pupils, staff, Parents) to consider improvements to the School's processes under the policy	Deputy Head: Pastoral	As required, and at least annually
Formal annual review	Proprietor	Annually

7 Role of staff and parents

7.1 Head and Senior Leadership Team

7.1.1 The Head has overall executive responsibility for the safety and welfare of members of the School community, including ensuring that there are appropriate filtering and monitoring systems in place to safeguard pupils.

7.1.2 The Designated Safeguarding Lead is the senior member of staff from the School's leadership team with lead responsibility for safeguarding and child protection, including online safety. The responsibility of the Designated Safeguarding Lead includes managing safeguarding incidents involving the use of technology in the same way as other safeguarding matters, in accordance with the School's child protection and safeguarding policy and procedures. The Designated Safeguarding Lead may delegate their day-to-day activities to a Deputy DSL as appropriate, however, the ultimate lead responsibility for child protection, remains with the designated safeguarding lead.

7.1.3 The Designated Safeguarding Lead will work with the IT Manager (see below) in monitoring technology uses and practices across the School and assessing whether any improvements can be made to ensure the online safety and well-being of pupils.

7.1.4 The Designated Safeguarding Lead will regularly monitor the technology incident log maintained by the IT Manager and designated filtering and monitoring officer.

7.1.5 The Designated Safeguarding Lead will regularly update other members of the School's Senior Leadership Team on the operation of the School's safeguarding arrangements, including online safety practices.

7.2 IT Manager

7.2.1 The IT Manager, together with his team, is responsible for the effective operation of the School's filtering system so that pupils and staff are unable to access any material that poses a safeguarding risk, including terrorist and extremist material, while using the School's network.

7.2.2 The IT Manager is responsible for ensuring that:

(a) the School's technology infrastructure is secure and, so far as is possible, is not open to misuse or malicious attack;

(b) the user may only use the School's technology if they are properly authenticated and authorised;

(c) the School has an effective filtering and monitoring policy in place and that it is applied and updated on a regular basis;

(d) the risks of pupils and staff circumventing the safeguards put in place by the School are minimised;

(e) the use of the School's technology is regularly monitored to ensure compliance with this policy and that any misuse or attempted misuse can be identified and reported to the appropriate person for investigation; and

(f) monitoring software and systems are kept up to date to allow the ICT team to monitor the use of email and the internet over the School's network and maintain logs of such usage.

7.2.3 Technical provision and safeguards are in place to filter and monitor inappropriate content as set out in 8.6.2. The IT Manager will report regularly to the Designated Safeguarding Lead on the operation of the School's technology. If the IT Manager has concerns about the functionality, effectiveness, suitability or use of technology within the School, including of the monitoring and filtering systems in place, he/she will escalate those concerns promptly to the Designated Safeguarding Lead.

7.2.4 The IT Manager is responsible for maintaining the technology incident log (a central record of all serious incidents involving the use of technology) and bringing any matters of safeguarding concern to the attention of the Designated Safeguarding Lead in accordance with the School's child protection and safeguarding policy and procedures.

7.3 All staff

7.3.1 All staff have a responsibility to act as good role models in their use of technology and to share their knowledge of the School's policies and of safe practice with the pupils.

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

7.3.3 All staff are aware that technology can play a significant part in many safeguarding and wellbeing issues and that pupils are at risk of abuse online as well as face-to-face. Staff are also aware that, sometimes, such abuse will take place concurrently online and during a pupil's daily life.

7.3.4 Staff are expected to be alert to the possibility of pupils abusing their peers online and to understand that this can occur both inside and outside of school. Examples of such abuse can include:

(a) the sending of abusive, harassing and misogynistic messages;

(b) the consensual and non-consensual sharing of indecent images and videos (especially around group chats), which is sometimes known as sexting or youth produced sexual imagery;

(c) the sharing of abusive images and pornography to those who do not wish to receive such content;

(d) cyberbullying.

7.3.5 Staff are also aware that many other forms of abuse may include an online element, through regular CPD and INSET. For instance, there may be an online element which:

(a) facilitates, threatens and / or encourages physical abuse;

(b) facilitates, threatens and / or encourages sexual violence; or

(c) is used as part of initiation / hazing type violence and rituals.

7.3.6 It is important that staff recognise the indicators and signs of child-on-child abuse, including where such abuse takes place online, and that they know how to identify it and respond to reports. Staff must also understand that, even if there are no reports of child-on-child abuse at the School, whether online or otherwise, it does not mean that it is not happening; it may simply be the case that it is not being reported.

7.3.7 It is important that staff challenge inappropriate behaviours between peers and do not downplay certain behaviours, including sexual violence and sexual harassment, as "*just banter*", "*just having a laugh*", "*part of growing up*" or "*boys being boys*" as doing so can result in a culture of unacceptable behaviours, an unsafe environment for children and, in a worst-case scenario, a culture that normalises abuse. The School has a **zero-tolerance approach** towards child-on-child abuse (including in relation 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.

7.3.8 Staff have a responsibility to report any concerns about a pupil's welfare and safety in accordance with this policy and the School's child protection and safeguarding policy and procedures. If staff have any concerns regarding child-on-child abuse or if they are unsure as to how to proceed in relation to a particular incident, they should **always speak to the Designated Safeguarding Lead in all cases**.

7.4 Parents

7.4.1 The role of parents in ensuring that pupils understand how to stay safe when using technology is crucial. The School expects parents to promote safe practice when using technology and to:

(a) support the School in the implementation of this policy and report any concerns in line with the School's policies and procedures;

(b) talk to their child to understand the ways in which they are using the internet, social media and their mobile devices and promote responsible behaviour; and

(c) encourage their child to speak to someone if they are being bullied or otherwise are concerned about their own safety or that of another pupil or need support.

7.4.2 If parents have any concerns or require any information about online safety, they should contact the Designated Safeguarding Lead or Deputy Head: Pastoral.

8 Access to the School's technology

8.1 The School provides internet, intranet and social media access and an email system to pupils and staff as well as other technology. Pupils and staff must comply with the respective acceptable use policy when using School technology. All such use is monitored by the ICT team.

8.2 Pupils and staff require individual usernames and passwords to access the School's internet, intranet and social media sites and email system which must not be disclosed to any other person. Any pupil or member of staff who has a problem with their usernames or passwords must report it to the ICT team immediately.

8.3 No laptop or other mobile electronic device may be connected to the School network without the consent of the Director of Finance and Administration/ IT Manager. The use of any device connected to the School's network will be logged and monitored by the ICT team. See also 8.5 below and the School's ICT Acceptable Use Policy.

8.4 The School has a separate Wi-Fi connection available for use by visitors to the School. A password, which is changed on a regular basis, must be obtained from a member of staff in order to use the Wi-Fi. Use of this service will be logged and monitored by the ICT team.

8.5 Inappropriate material

8.5.1 The School recognises the importance of ensuring that all pupils are safeguarded from potentially harmful and inappropriate material online.

8.5.2 Online safety is a key element of many school policies and procedures and an important part of the role and responsibilities of the Designated Safeguarding Lead (KCSIE, 2025) in relation to filtering and monitoring guidelines. The term 'online safety' encapsulates a wide range of issues, but these can be classified into four main areas of risk:

(a) **Content** - being exposed to illegal, inappropriate or harmful content (e.g. pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism);

(b) **Contact** - being subjected to harmful online interaction with other users (e.g. peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom and / or exploit them for sexual, criminal, financial or other purposes);

(c) **Conduct** - a pupil's personal online behaviour that increases the likelihood of, or causes, harm (e.g. making, sending and receiving explicit images (such as consensual and non-consensual sharing of nudes and semi-nudes and / or pornography), sharing other explicit images and online bullying; and

(d) **Commerce** - risks such as online gambling, inappropriate advertising, phishing and or financial scams.

8.6 Use of mobile electronic devices and smart technology

8.6.1 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. Mobile devices and smart technology equipped with a mobile data subscription can, however, provide pupils with unlimited and unrestricted access to the internet. The School is alert to the risks that such access presents, including the risk of pupils sexually harassing their peers using their mobile or other smart technology; or sharing indecent images consensually or non-consensually; or viewing and / or sharing pornography and other harmful content, and has mechanisms in place to manage such risks.

8.6.2 As per The Mobiles Phones in School (2024) DfE Guidance, the school prohibits the use of mobile phones in school.

8.6.3 E-safety control measures

(a) The School provides internet, intranet and social media access and an email system to pupils and staff as well as other technology. Pupils and staff must comply with the respective acceptable use policy when using School technology. All such use is monitored by the ICT team/Deputy Head: Pastoral.

(b) The School's policies apply to the use of technology by staff and pupils whether on or off School premises and appropriate action will be taken where such use affects the welfare of other pupils or any member of the School community or where the culture or reputation of the School is put at risk.

(c) **Internet access:**

(i) Internet access will be authorised once parents and pupils have returned the signed consent form in line with our Acceptable Use Agreement.

(ii) Where a pupil is over the age of 13 and they fully understand what they are consenting to, parents' consent is not required in line with the GDPR; however, the school will notify parents that the pupil has consented independently.

(iii) A record will be kept by the IT Manager of all pupils who have been granted internet access.

(iv) All users in KS3 and above will be provided with usernames and passwords and will be instructed to keep these confidential to avoid any other pupils using their login details.

(v) Pupils' passwords will expire every 90 days, and their activity is continuously monitored by the Deputy Head: Pastoral.

(vi) Management systems will be in place to allow teachers and members of staff to control workstations and monitor pupils' activity.

(vii) Effective filtering systems will be established to eradicate any potential risks to pupils through access to, or trying to access, certain websites which are harmful or use inappropriate material.

(viii) Filtering systems will be used which are relevant to pupils' age ranges, their frequency of use of ICT systems, and the proportionality of costs compared to risks.

(ix) The Deputy Head: Pastoral will ensure that the use of appropriate filters and monitoring systems does not lead to 'over blocking' – unreasonable restrictions as to what pupils can be taught with regards to online teaching and safeguarding.

(x) Any requests by staff for websites to be added or removed from the filtering list must be first authorised by the IT Manager and may be referred to the Deputy Head: Pastoral.

(xi) All school systems will be protected by up-to-date virus software.

(xii) An agreed procedure will be in place for the provision of temporary users, e.g. volunteers.

(xiii) Staff are able to use the internet for personal use during out-of-school hours, as well as break and lunch times.

(xiv) Personal use will only be monitored by either the Deputy Head, Pastoral or the Director of Strategy and Innovation, in conjunction with the IT Manager for access to any inappropriate or explicit sites, where the need to do so outweighs the need for privacy.

(xv) Inappropriate internet access by staff may result in the staff member being permitted to use the internet for school purposes only and prohibited from using any personal devices. This will be dealt with following the process outlined in the misuse by staff section of this policy.

(d) **Email:**

(i) Pupils and staff will be given approved email accounts and are only able to use these accounts.

(ii) The use of personal email accounts to send and receive personal data or information is prohibited.

(iii) No sensitive personal data shall be sent to any other pupils, staff or third parties via email.

(iv) Pupils are made aware that all email messages are monitored, and that the filtering system will detect inappropriate links, viruses, malware and profanity.

(v) Staff members are aware that their email messages are not monitored but can be viewed, if required.

(vi) Any emails sent by pupils to external organisations will be overseen by their class teacher and must be authorised before sending.

(vii) Chain letters, spam and all other emails from unknown sources will be deleted without opening.

(viii) The heads of year will, during the school year hold an assembly or arrange a PSHE lesson explaining what a phishing email might look like – this assembly will include information on the following:

(A) Determining whether or not an email address is legitimate

(B) Knowing the types of address a phishing email could use

(C) Asking “does it urge the recipient to act immediately?”

(D) Checking the spelling and grammar

(ix) Staff will not be subject to disciplinary action if they are caught out by cyber-attacks as this may prevent similar reports in the future. The Director Finance will conduct an investigation; however, this will be to identify the cause of the attack, any compromised data and if there are any steps that can be taken in the future to prevent similar attacks happening.

(e) Social networking:

(i) The use of social media on behalf of the school will be conducted following the processes outlined in our Data Protection and ICT Acceptable for Staff policy and ICT Acceptable use Policy for Students.

(ii) Access to social networking sites will be filtered as appropriate.

(iii) Pupils are regularly educated on the implications of posting personal data online outside of the school.

(iv) Staff are regularly educated on posting inappropriate photos or information online, which may potentially affect their position and the school as a whole.

(v) Staff are not permitted to communicate with pupils over social networking sites and are reminded to alter their privacy settings.

(vi) Staff are not permitted to publish comments about the school which may affect its reputation.

(vii) Staff are not permitted to access social media sites during teaching hours unless it is beneficial to the material being taught.

(f) **Published content on the school website:**

(i) The Head will be responsible for the overall content of the website and will ensure the content is appropriate and accurate.

(ii) Contact details on the school website will include the phone number, email and address of the school – no personal details of staff or pupils will be published.

(iii) Images and full names of pupils, or any content that may easily identify a pupil, will be selected carefully and will not be posted until authorisation from parents has been received.

(iv) Pupils are not permitted to take or publish photos of others without permission from the individual.

(v) Staff are able to take pictures, though they must do so in accordance with our Camera Use Policy. Staff will not take pictures using their personal equipment.

(vi) Any member of staff that is representing the school online, e.g. through blogging, must express neutral opinions and not disclose any confidential information regarding the school, or any information that may affect its reputability.

(g) **Mobile devices and hand-held computers:**

(i) Students are allowed to connect their personal devices to the school Wi-Fi network. The use of any device connected to the School's Wi-Fi network will be logged and monitored by the ICT team.

(ii) Year 7- 10 will hand in their phones at the start of the school day.

(iii) Year 11 and above may use mobile phones during lessons at the discretion of the teacher and for the following purposes:

(A) To research for educational purposes using the internet

(B) To take a photograph of an artefact produced

(C) To record a presentation, interview or small group activity

(D) To look up a word using an on-line dictionary or dictionary app

(E) To use the calculator function

(F) To read an eBook

(iv) Approved devices must be in silent mode while on school campus, unless otherwise allowed by a teacher. Headphones may be used with teacher permission.

(v) Pupil access to the school internet is limited at certain times of the day as per the ICT policy.

(vi) Students and parents/guardians participating in the schools Bring Your Own Device scheme must adhere to the ICT Acceptable Use for Students.

(vii) Staff and students may not use mobiles devices in the school corridors.

(viii) Staff in our BYOD scheme must adhere to the Staff Handbook and Data Protection and ICT Acceptable Use Policy for Staff and Camera Use Policy. Internet access will be logged for investigating any inappropriate use by the Deputy Head: Pastoral where it is justifiable to do so and the justification outweighs the need for privacy.

(ix) The sending of inappropriate messages or images from mobile devices is prohibited.

(x) The DPO will, in collaboration with the IT Manager, ensure all school-owned devices are password protected and encrypted.

(xi) To protect, retrieve and erase personal data, all mobile devices and hand-held computers will be fitted with software to ensure they can be remotely wiped.

(xii) The IT Manager will review all mobile devices and hand-held computers on a termly basis to ensure all apps are compliant with data protection regulations and up-to-date, and to carry out any required updates.

(xiii) The IT Manager will review and authorise any apps and/or computer programmes before they are downloaded to school owned devices and where necessary seek further approval from the ST. – no apps or programmes will be downloaded onto a school owned device without express permission from an IT Manager.

(xiv) Mobile device apps will only be downloaded from manufacturer approved stores, e.g. Google Play and the Apple App Store.

(xv) The school's network filters will be applied to a device's connection to the internet and any attempt to bypass the network filters is prohibited.

(h) **Network security:**

(i) Network profiles for each pupil and staff member are created in which the individual must enter a username and personal password when accessing the ICT systems within the school.

(ii) Passwords have a minimum and maximum length, to prevent 'easy' passwords or mistakes when creating passwords.

(iii) Passwords will require a mixture of letters, numbers and symbols to ensure they are secure as possible.

(iv) Passwords will expire after 90 days to ensure maximum security for pupil and staff accounts.

(v) Passwords should be stored using non-reversible encryption.

(vi) The following passwords will not be accepted by the school's security systems as they are too predictable:

(A) Password

(B) Pa55word

(C) Password123

(D) Qwerty

(E) 123456

(F) 12345678

(vii) The IT Manager will ensure all school-owned laptops and computers have their encryption settings turned on or, if there is no built-in encryption option, encryption software is installed.

(viii) Important folders, e.g. those including pupils' medical records, will be protected to ensure their security – the Deputy Head: Pastoral, school nurse and other designated individual(s) will be the only people who have access to these files.

(i) **Virus management:**

(i) Technical security features, such as virus software, are kept up-to-date and managed by the IT Manager.

(ii) The IT Manager will ensure that the filtering of websites and downloads is up-to-date and monitored.

(iii) Firewalls will be switched on at all times – The IT Manager will review these on a weekly basis to ensure they are running correctly and to carry out any required updates.

(iv) Firewalls and other virus management systems, e.g. anti-virus software, will be maintained in accordance with the school's Data Breach Policy and Procedure.

(v) Staff members will report all malware and virus attacks to the IT Manager immediately.

8.6.4 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. Permission to do so must be sought and given in advance.

8.6.5 The School rules about the use of mobile electronic devices or other smart technology, including access to open / non-School networks, are set out in the acceptable use policy for pupils.

8.6.6 The use of mobile electronic devices by staff is covered in the staff code of conduct and the IT acceptable use policy for staff. We recommend in the first instance that staff make use of the School's 'Remote Desktop' facility whenever possible and at all times minimize the amount of data that is held on personal devices.

8.6.7 The School's policies apply to the use of technology by staff and pupils whether on or off School premises and appropriate action will be taken where such use affects the welfare of other pupils or any member of the School community or where the culture or reputation of the School is put at risk.

8.7 Use of Generative AI Tools

8.7.1 The School recognises the educational potential and safeguarding risks associated with generative AI tools (e.g. chatbots, image generators, content creators).

8.7.2 Pupils may only use generative AI tools under staff supervision and via school-approved platforms.

8.7.3 Staff must ensure that any use of generative AI aligns with the School's safeguarding, data protection, and acceptable use policies.

8.7.4 The use of generative AI for cheating, harassment, misinformation, or other harmful purposes is strictly prohibited and will be treated as a breach of discipline and safeguarding.

8.7.5 The IT Manager will ensure filtering systems block access to generative AI tools that lack appropriate safety controls or violate age restrictions.

9 Procedures for dealing with incidents of misuse

9.1 Staff, pupils and parents are required to report incidents of misuse or suspected misuse to the School in accordance with this policy and the School's safeguarding and disciplinary policies and procedures.

9.2 The School recognises the importance of acknowledging, understanding and not downplaying behaviours which may be related to abuse and has appropriate systems in place to ensure that pupils can report any incidents of abuse, whether or not they include an online element, confidently and safe in the knowledge that their concerns will be treated seriously. Staff should however be careful not to promise that a concern will be dealt with confidentially at an early stage as information may need to shared further (e.g. with the Designated Safeguarding Lead) to discuss next steps.

9.3 Misuse by pupils

9.3.1 Anyone who has any concern about the misuse of technology by pupils should report it immediately so that it can be dealt with in accordance with the School's behaviour and discipline policies, including the anti-bullying policy where there is an allegation of cyberbullying.

Type of misuse	Relevant policy	Reporting channel
Bullying	Preventing and Tackling Bullying	Housemistress, Form Tutor / Head of Year Note any incidents which give rise to safeguarding concerns must be referred on to the Designated Safeguarding Lead
Sharing nudes and semi-nude images (sexting / youth produced sexual imagery)	Safeguarding and child protection policy	Housemaster / Housemistress, Form Tutor / Head of Year Who should then refer to the Designated Safeguarding Lead who has overall responsibility for online safety matters
Sexual violence and sexual harassment (whether during or outside of school)	Safeguarding and child protection policy	The Designated Safeguarding Lead who has overall responsibility for online safety matters
Harassment	Safeguarding and child protection policy	Housemistress / Form Tutor / Head of Year

		Who should then refer to the Designated Safeguarding Lead who has overall responsibility for online safety matters
Upskirting	Safeguarding and child protection policy	Housemistress / Form Tutor/Head of Year Who should then refer to the Designated Safeguarding Lead who has overall responsibility for online safety matters
Radicalisation	Safeguarding and child protection policy	Housemistress / Form Tutor/Head of Year Who should then refer to the Designated Safeguarding Lead who has overall responsibility for online safety matters
Other breach of acceptable use policy	See relevant policy referred to in acceptable use policy	Housemistress / Form Tutor / Head of Year Who should then refer to the Designated Safeguarding Lead who has overall responsibility for online safety matters

Misuse of generative AI tools, including the creation or sharing of harmful, misleading, or inappropriate content, will be treated as a safeguarding concern and addressed under the School's behaviour and safeguarding policies

9.3.2 **Anyone** who has **any** concern about the welfare and safety of a pupil must report it **immediately** in accordance with the School's child protection procedures (see the School's child protection and safeguarding policy and procedures).

9.4 **Misuse by staff**

9.4.1 Anyone who has any concern about the misuse of technology by staff should report it in accordance with the School's whistleblowing policy so that it can be dealt with in accordance with the staff disciplinary procedures.

9.4.2 If anyone has a safeguarding-related concern relating to staff misuse of technology, they should be report it immediately so that it can be dealt with in accordance with the procedures for reporting and dealing with allegations of abuse against staff set out in the School's child protection and safeguarding policy and procedures.

9.4.3 Staff misuse of generative AI tools, including the generation or dissemination of inappropriate or misleading content, must be reported and will be investigated under the School's disciplinary and safeguarding procedures.

9.5 **Misuse by any user**

9.5.1 Anyone who has any concern about the misuse of technology by any other user should report it immediately to the IT Manager or the Designated Safeguarding Lead.

9.5.2 The School reserves the right to withdraw access to the School's network by any user at any time and to report suspected illegal activity to the police.

9.5.3 If the School considers that any person is vulnerable to radicalisation, the school will refer this to the Channel programme. This focuses on support at an early stage to people who are identified as being vulnerable to being drawn into terrorism. Any person who has a concern relating to extremism may report it directly to the police.

10 Education

10.1 The safe use of technology is integral to the School's curriculum. Pupils are educated in an age-appropriate manner about the importance of safe and responsible use of technology, including the internet, social media and mobile electronic devices (see the School's curriculum policy).

10.2 The safe use of technology is a focus in all areas of the curriculum and teacher training, and key safety messages are reinforced as part of assemblies and tutorial / pastoral activities, teaching pupils:

10.2.1 about the risks associated with using the technology and how to protect themselves and their peers from potential risks;

10.2.2 about the importance of identifying, addressing and reporting inappropriate behaviour, whether on or offline, and the risks of downplaying such behaviour as, for example, "*banter*" or "*just boys being boys*";

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

10.2.4 how to recognise suspicious, bullying or extremist behaviour;

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

10.2.6 the consequences of negative online behaviour;

10.2.7 how to report cyberbullying and / or incidents that make pupils feel uncomfortable or under threat and how the School will deal with those who behave badly; and

10.2.8 how to respond to harmful online challenges and hoaxes.

10.2.9 pupils will be taught about the ethical use of generative AI, including how to critically evaluate AI-generated content and understand the risks of misinformation, deepfakes, and inappropriate use.

10.3 Pupils are also taught about the risks associated with all forms of abuse, including physical abuse and sexual violence and sexual harassment which may include an online element. The School has 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.

10.4 Pupils are instructed to report any suspicious use of the internet and digital devices to their Head of Year, Housemistress, Form Tutor or Teachers.

10.5 PSHE lessons will be used to educate pupils about cyber bullying, including how to recognise and report cyber bullying, the social effects of spending too much time online and where to access help and how the School will deal with those who behave badly.

10.6 The school will hold e-safety events, such as Safer Internet Day and Anti-Bullying Week, to promote online safety.

10.7 Those parts of the curriculum which deal with the safe use of technology are reviewed on a regular basis to ensure their relevance.

10.8 The School's acceptable use policy for pupils sets out the School rules about the use technology including internet, email, social media and mobile electronic devices, helping pupils to protect themselves and others when using technology. Pupils are reminded of the importance of this policy on a regular basis.

10.9 **Useful online safety resources for pupils**

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

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

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

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

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

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

10.9.7 https://www.bbc.com/ownit

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

11 Training

11.1 Staff

11.1.1 All staff will employ methods of good practice and act as role models for pupils when using the internet and other digital devices.

11.1.2 The School provides training on the safe use of technology to staff so that they are aware of how to protect pupils and themselves from the risks of using technology and to deal appropriately with incidents involving the use of technology when they occur.

11.1.3 Induction training for new staff includes training on the School's online safety strategy including this policy, the staff code of conduct and the ICT acceptable use policy. Ongoing staff development training includes training on technology safety together with specific safeguarding issues including sharing nudes and semi-nudes images and or videos or via live stream, cyberbullying, radicalisation and dealing with harmful online challenges and online hoaxes.

11.1.4 Where pupils wish to report a safeguarding concern, all staff are taught to reassure victims that they are being taken seriously and that they will be supported and kept safe. Staff are aware of the importance of their role in dealing with safeguarding and wellbeing issues, including those involving the use of technology, and understand that a victim should never be given the impression that they are creating a problem by reporting abuse, including sexual violence or sexual harassment, and nor should they ever be made to feel ashamed for making a report.

11.1.5 Where safeguarding incidents involve an online element, such as youth produced sexual imagery, staff will not view or forward sexual imagery reported to them and will follow the School's policy on sharing nudes and semi-nude images and videos as set out in Appendix 1 of the School's Safeguarding and Child Protection Policy and Procedures and Searching, screening and confiscation: advice for schools (DfE, July 2022) and filtering and monitoring update (KCSIE 2025). In certain cases, it may be appropriate for staff to confiscate a pupil's devices to preserve any evidence and hand it to the police for inspection.

11.1.6 Staff are encouraged to adopt and maintain an attitude of 'it could happen here' in relation to sexual violence and sexual harassment and to address inappropriate behaviours (even where such behaviour appears relatively innocuous) as this can be an important means of intervention to help prevent problematic, abusive and / or violent behaviour in the future.

11.1.7 Staff are trained to look out for potential patterns of concerning, problematic or inappropriate behaviour and, where a pattern is identified, the School will decide on an appropriate course of action to take. Consideration will also be given as to whether there are wider cultural issues within the School that facilitated the occurrence of the inappropriate behaviour and, where appropriate, extra teaching time and / or staff training will be delivered to minimise the risk of it happening again.

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

11.1.9 The frequency, level and focus of all such training will depend on individual roles and requirements and will be provided as part of the School's overarching approach to safeguarding.

11.1.10 **Useful online safety resources for staff**

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

(b) https://www.saferinternet.org.uk/advice-centre/teachers-and-professionals

(c) http://www.childnet.com/teachers-and-professionals

(d) https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online-safety/

(e) https://www.thinkuknow.co.uk/teachers/

(f) http://educateagainsthate.com/

(g) https://www.commonsense.org/education/

(h) Cyberbullying: advice for head teachers and school staff (DfE, November 2014)

(i) Advice on the use of social media for online radicalisation (DfE and Home Office, July 2015)

(j) Sharing nudes and semi-nudes: advice for education settings working with children and young people (UKCIS, March 2024).

(k) Online safety in schools and colleges: questions from the governing board (UKCIS, 2022)

(l) Education for a connected world framework (UKCIS, 2020)

(m) https://www.lgfl.net/online-safety/resource-centre

(n) Online Sexual Harassment: Understand, Prevent and Respond Guidance for Schools (Childnet, March 2019)

(o) Myth vs Reality: PSHE toolkit (Childnet, April 2019)

(p) SELMA Hack online hate toolkit (SWGFL, May 2019)

(q) Teaching online safety in school: Guidance supporting schools to teach their pupils how to stay safe online, within new and existing school subjects (DfE, June 2019)

(r) Harmful online challenges and online hoaxes (DfE, February 2021)

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

(t) NSPCC helpline for anyone worried about a child - 0808 800 5000

(u) Internet Watch Foundation - internet hotline for the public and IT professionals to report potentially criminal online content

11.1.11 The Brighton & Hove Safeguarding Children Partnership (BHSCP) has produced guidance for parents on radicalisation which is available here: https://www.bhscp.org.uk/preventing-abuse-and-neglect/spotting-the-signs/signs-of-radicalisation-extremism/

11.1.12 The Deputy Head: Pastoral will act as the first point of contact for staff requiring e-safety advice.

11.1.13 Staff training will include awareness of generative AI risks and safe practices, including how to supervise pupil use and respond to incidents involving AI-generated content.

11.2 Parents

11.2.1 Parents are encouraged to read the acceptable use policy for pupils with their daughter to ensure that it is fully understood.

11.2.2 E-safety information will be directly delivered to parents through the parent bulletin. The parent bulletin will contain regular and relevant online safety resources aimed at parents, including various digital resources such as posters and webinars.

11.2.3 Parent meetings occasions will be utilised to inform parents of any e-safety related concerns.

11.2.4 **Useful online safety resources for parents**

(a) https://www.saferinternet.org.uk/advice-centre/parents-and-carers

(b) http://www.childnet.com/parents-and-carers

(c) https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online-safety/

(d) https://www.thinkuknow.co.uk/parents/

(e) http://parentinfo.org/

(f) http://parentzone.org.uk/

(g) https://www.net-aware.org.uk

(h) https://www.internetmatters.org/

(i) https://www.commonsensemedia.org/

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

(k) http://www.askaboutgames.com

(l) https://www.ceop.police.uk/safety-centre

(m) UK Chief Medical Officers' advice for parents and carers on children and young people's screen and social media use (February 2019)

(n) LGfL: parents - scare or prepare

(o) Thinkuknow: what to do if there's a viral scare online

12 Cybercrime

12.1 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).

12.2 12.2 Cyber-dependent crimes include:

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

12.2.2 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

12.2.3 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.

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

12.4 If staff have any concerns about a child in this area, they should refer the matter to the Designated Safeguarding Lead immediately. The Designated Safeguarding Lead should 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. It aims to intervene where young people are at risk of committing, or being drawn into, low level cyber-dependent offences and divert them to a more positive use of their skills and interests. Cyber Choices does not currently cover 'cyber-enabled' crime such as fraud, purchasing of illegal drugs on-line and child sexual abuse and exploitation, nor other areas of concern such as on-line bullying or general on-line safety.

13 Risk assessment

13.1 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.

13.2 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.

13.3 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.

13.4 Day to day responsibility to carry out risk assessments under this policy will be delegated to Heads of Year and Housemistresses.

14 Record keeping

14.1 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.

14.2 All serious incidents involving the use of technology will be logged centrally in the technology incident log by the IT Manager.

14.3 The records created in accordance with this policy may contain personal data. The School has a number of privacy notices which explain how the School will use personal data. The School's approach to data protection compliance is set out in the data protection and ICT acceptable use policy. In addition, staff must ensure that they follow the School's data protection policies and procedures when handling personal data created in connection with this policy; this includes the School's ICT Acceptable use policy.

15 Version control

Date of adoption of this policy	September 2025
Date of last review of this policy	September 2025
Date for next review of this policy	September 2026
Policy owner (SMT)	Designated Safeguarding Lead
[Policy owner (Proprietor)]	Council of Trustees, Roedean School