Policy No: 14

THE ROCHE SCHOOL

SAFEGUARDING CHILDREN – ONLINE SAFETY POLICY

This policy, which applies to the whole school, is publicly available on the school website and upon request a copy (which can be made available in large print or other accessible format if required) may be obtained from the School Office.

Document Details:

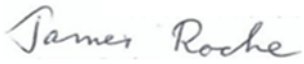
Scope: All who work, volunteer or supply services to our school have an equal responsibility to understand and implement this policy and its procedures both within and outside of normal school hours, including activities away from school. All new employees and volunteers are required to state that they have read, understood and will abide by this policy and its procedural documents and confirm this by signing the *Policies Register*.

Legal Status: Complies with The Education (Independent School Standards) (England) Regulations currently in force.

Monitoring and Review: These arrangements are subject to continuous monitoring, refinement, and audit by the Headteacher. The Proprietor and Advisory Board will undertake a full annual review of this document, inclusive of its implementation and the efficiency with which the related duties have been implemented. This review will be formally documented in writing. Any deficiencies or weaknesses recognised in arrangements or procedures will be remedied immediately and without delay. All staff will be informed of the updated/reviewed arrangements and it will be made available to them in writing or electronically.

Signed: Signed:

Date reviewed: October 25



Date of next review: October 2026

Charlotte Doherty
Headteacher

James Roche
Proprietor

Introduction: The purpose of this Policy is to safeguard pupils and staff at The Roche School. It details the actions and behaviour required from pupils and members of staff in order to maintain a safe electronic environment and is based on current best practice drawn from a wide range of sources. In accordance with legislative requirements we have a whole school approach to Online Safety. Our key message to keep pupils and young people safe is to be promoted and should be applied to both online and offline behaviours. Within our Online Safety policy, we have clearly defined roles and responsibilities for online safety as part of the school's wider safeguarding strategy and how this links with our main Safeguarding (Child Protection) Policy and other related documents.

Online safety is a running and interrelated theme when devising and implementing our wider school policies and procedures, including our Safeguarding & Child Protection Policy and our Preventing Extremism and Tackling Radicalisation Policy. The staff and pupil Acceptable Use Policies (AUPs) are central to the Online Safety policy and should be consulted alongside this policy.

We consider how we can promote online safety whilst developing our curriculum, through our staff training, and also through parental engagement. The Online Safety policy will be reviewed annually by the safeguarding team who will provide recommendations for updating the policy in the light of experience and changes in legislation or technologies. The Pupil Council will be consulted regarding any changes to the Pupil AUP. All staff should read these policies in conjunction with the Online Safety policy. This is particularly important with regard to the Prevent Strategy, as a large portion of cases of radicalisation happen through the online medium. Staff must be vigilant when dealing with such matters and ensure that they observe the procedure for reporting

such concerns in line with that laid out in the Safeguarding (Child Protection) Policy, Preventing Extremism and Tackling Radicalisation Policy.

Legislation and guidance

- Part 3, paragraphs 7 (a) and (b) of the Education (Independent School Standards) (England) Regulations 2014, in force from the 5th January 2015 and as amended in September 2015
- *Keeping Students Safe in Education* (KCSIE) *Information for all schools and Colleges* (DfE: September 2023) incorporates the additional statutory guidance,
- *Disqualification under the Childcare Act 2006 Childcare (Disqualification) and Childcare (Early Years Provision Free of Charge) (Extended Entitlement) (Amendment) Regulations 2018.*
- *Working Together to Safeguard Students* (WT) (HM Government: September 2018) which also refers to non-statutory advice, *Information sharing* HM Government: March 2015); *Prevent Duty Guidance: for England and Wales* (2021) (*Prevent*). *Prevent* is supplemented by *The Prevent duty: Departmentaladvice for Schools and childminders (June 2015)* and
- Based on guidance from the DfE (2014) 'Cyberbullying: Advice for Heads and School staff 'and 'Advice for parents and carers on cyberbullying'
- Prepared with reference to DfE Guidance (2014) *Preventing and Tackling Bullying: Advice for School leaders and governors* and the relevant aspects of *Safe to Learn, embedding anti-bullying work in Schools.*
- Having regard for the guidance set out in the DfE *(Don't Suffer in Silence booklet)*
- The Data Protection Act 1998; GDPR, 2018; BECTA and CEOP.
- Teaching Online Safety in Schools (DfE: 2023)
- The policy also takes into account the National Curriculum computing programmes of study.
- Meeting digital and technology standards in Schools and Colleges (DfE: 2023) (including Broadband, Cyber-Security and data protection procedures)
- Filtering and monitoring standards for schools and colleges (DfE: 2023)
- Cyber security standards for schools and colleges (DfE: 2023)
- Promoting and supporting mental health and wellbeing in schools and colleges (September 2022)
- Behaviour in schools (September 2022)

Guidance (UK Safer Internet Centre)

- 2023 Appropriate filtering and monitoring definitions published (UK Safer Internet Centre)
- Test Your Internet Filter (UKSIC / SWGfL)
- A Guide for education settings and filtering providers (UKCIS)
- Establishing appropriate levels of filtering (UKSIC)
- Online safety in schools and colleges: questions from the governing board (UKCIS)

Roles and responsibilities: Our Head of Safeguarding (and Senior DSL), working in conjunction with our IT managers, is responsible for ensuring the online safety of the school community. Our IT Manager will take operational responsibility for online safety in the School, but the overall responsibility will fall on the senior DSL for making sure that policy is enforced and that the necessary checks, filters and monitoring are in place. It is the school responsibility to ensure that students are safe from cyber bullying both within and outside the school community and that appropriate steps are taken if an incident occurs. The Leadership Team will also review online safety and the acceptable use of technology in the school during their regular meetings and ensure that:

- pupils know how to use the Internet responsibly and that parents and teachers have the right measures in place to keep pupils safe from exploitation or radicalisation.
- pupils are safe from terrorist and extremist material when accessing the Internet in school, including by establishing appropriate levels of filtering.
- pupils use Information and Communications Technology (ICT) safely and securely and are aware of both external and peer to peer risks when using ICT, including cyberbullying and other forms of abuse.
- children, staff, the Advisory Board and volunteers will receive the appropriate Online Safety training, guidance, time and resources to effectively implement online safety policies and procedures;

- clear and rigorous policies and procedures are to be applied to the use/non-use of personal ICT equipment by all individuals who affect or come into contact with the early years setting. Such policies and procedures are to include the personal use of work-related resources.
- the Acceptable Use Policies (AUPs) are to be implemented, monitored and reviewed regularly, and for ensuring all updates are to be shared with relevant individuals at the earliest opportunity.
- monitoring procedures are to be transparent and updated as agreed in school policies.
- allegations of misuse or known incidents are to be dealt with appropriately and promptly, in line with agreed procedures, and in liaison with other agencies, where applicable.
- effective online safeguarding support systems are to be put in place, for example, filtering controls, secure networks and virus protection to ensure that the school's technical infrastructure is secure and is not open to misuse or malicious attack.
- an appropriate level of authorisation is to be given to ICT users. Not all levels of authorisation will be the same - this will depend on, for example, the position, work role and experience of the individual concerned.
- users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed.
- a current record of all staff and pupils who are granted access to school ICT system is maintained.

Designated Safeguarding Lead (DSL): The Designated Safeguarding Lead (DSL) is a senior member of the management team who has relevant, current and practical knowledge and understanding of safeguarding, child protection and online safety. Access to an individual holding this role is available at all times, for example, a Deputy Designated Safeguarding Lead is also in place should the DSL be absent. The designated persons for safeguarding will be responsible for ensuring that:

- agreed policies and procedures are to be implemented in practice.
- all updates, issues and concerns are to be communicated to all ICT users.
- Updating and delivering staff training on online safety which, amongst other things, includes an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring (appendix 3 contains a self-audit for staff on online safety training needs.
- the importance of online safety in relation to safeguarding is to be understood by all ICT users.
- the training, learning and development requirements of staff are to be monitored and additional training needs identified and provided for.
- the learning and development plans of pupils and young people will address online safety.
- a safe ICT learning environment is to be promoted and maintained.

Not all levels of authorisation will be the same - this will depend on, for example, the position, work role and experience of the individual concerned. In some instances, explicit individual authorisation must be obtained for specific activities when deemed appropriate, and any concerns and incidents are to be reported in a timely manner in line with agreed procedures. The learning and development plans of students and young people will address online safety. A safe ICT learning environment is to be promoted and maintained.

The Proprietor's responsibilities: Whilst considering their responsibility to safeguard and promote the welfare of children and provide them with a safe environment in which to learn, the proprietor will do all that they reasonably can to limit children's exposure to risks when using the school's IT system. As part of this process, the proprietor has ensured the school has appropriate filters and monitoring systems in place which are reviewed regularly to monitor their effectiveness. They ensure that the leadership team and relevant staff have an awareness and understanding of the provisions in place, how to manage them effectively and know how to escalate concerns when identified.

All Staff: It is the responsibility of all staff to be alert to possible harm to pupils or staff due to inappropriate Internet access or use, both inside and outside of The Roche School, and to deal with incidents of such as a priority. All staff are responsible for ensuring they are up to date with current online safety issues, and this online Safety Policy. Cyber-bullying incidents will be reported in accordance with The Roche School's Anti-Bullying Policy. All staff will ensure they understand and adhere to our staff Acceptable Use Policy, which they must sign and return to the Online Safety Officer which will be placed on staff

files. Teachers will ensure they are confident in promoting and delivering online safety as required, identifying risks and reporting concerns as they arise.

Parents/Carers: Parents/carers are responsible for ensuring their child understands how to use computer technology and other digital devices appropriately. The Roche School will support parents/carers by sharing information and links through our website, newsletters, social media platforms and regular safety briefings via email, raising any concerns that they have.

All Pupils: All pupils will ensure they understand and adhere to our pupil Acceptable Use Policy, which they must sign and return to the Online Safety Officer. Pupils are reminded of their responsibilities regarding the use of the school's ICT systems and equipment, including their expected behaviour.

Breadth of Online Safety Issues: We classify the issues within online safety into **four** areas of risk:

- **Content:** being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.
- **Contact:** being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
- **Conduct:** personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying; and
- **Commerce** - risks such as online gambling, inappropriate advertising, phishing and or financial scams.

The following is a list of possible risks students may face in their access to technology:

- Access to illegal, harmful or inappropriate images or content
- The risk of being subject to grooming by those whom they contact on the internet
- Inappropriate and unsafe communication with strangers
- Cyber bullying
- Access to pornographic material
- Access to extremist material that could lead to radicalisation of students
- Access to unsuitable video or gaming sites
- Sites that encourage gambling
- Illegal downloading of material that breaks copyright laws
- Unauthorised access to/loss of/sharing of personal information

The above risks can be realised through a wide range of technologies, including:

- e-mail
- Smart phones, tablets and laptops, etc.
- The Internet (web)
- Social networking sites; Twitter, YouTube, Facebook etc.
- Gaming sites
- Blogs, instant messaging, chat rooms, message boards, virtual learning environments
- Webcams, video hosting sites
- Photography

These issues are to be managed through the school's filtered Internet, by promoting safe and responsible use, and ensuring both staff and pupils are able to report any concerns to the appropriate people.

Staff/Volunteers' Use of IT Systems: Access to the Internet and e-mail is provided to support the curriculum, support school administration and for staff professional development only. All staff must read and confirm by signature that they have read the 'Staff Acceptable Use Policy' before using any school ICT resource. In addition:

- All staff including the Proprietor and Advisory Board will receive appropriate Online Safety training, which is updated regularly;
- Online Safety issues are embedded in all aspects of the curriculum and other activities.
- Access to systems should be made by authorised passwords, which must not be made available to any other person.
- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse, using personal data only on secure password-protected computers and other devices.
- In lessons where Internet use is pre-planned, pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in Internet searches.

- Where pupils are allowed to freely search the Internet, staff should be vigilant in monitoring the content of the websites the pupils visit.
- Occasionally pupils may need to research educational material that may normally result in websites being blocked (e.g. racism). In this situation, staff may request to remove these sites from the filtered list for the period of study. Any request to do so should be made to the IT Manager.
- The Internet can be used to actively gather personal information about individuals which may lead to undesirable consequences (e.g. SPAM, fraud, harassment or identity theft). Because of this, staff are advised to only use the school approved software and email systems which have appropriate security in place.
- Files should not be saved directly from the Internet unless they can first be scanned for computer viruses, malware, spyware and other malicious programmes;

Any person suspecting another of deliberate misuse or abuse of technology should take the following action:

1. Report in confidence to the school's member of staff who is responsible for online safety, who is the DSL
2. The Online Safety Officer should investigate the incident.
3. If this investigation results in confirmation of access to illegal material, the committing of illegal acts, or transgression of school rules, appropriate sanctions will be enforced.
4. In exceptional circumstances, where there are reasonable grounds to suspect that a user has committed a serious criminal offence, the Child Exploitation and Online Protection Command (CEOP) and the police will be informed.
5. No pupil or member of staff should attempt to access or view the material, whether online or stored on internal or external storage devices. If this step is necessary, CEOP and the police will be contacted.

Teaching about Online Safety:

Because new opportunities and challenges appear all the time, it is important that we focus our teaching on the underpinning knowledge and behaviours that can help pupils to navigate the online world safely and confidently regardless of the device, platform or app. Online Safety is a focus in all areas of the curriculum and key Online Safety messages are reinforced regularly, teaching pupils about the risks of Internet use, how to protect themselves and their peers from potential risks, how to recognise suspicious, bullying or extremist behaviour and the consequences of negative online behaviour. Our Online Safety Curriculum is closely linked with our Relationships and Sex Education Programme and discusses the links associated with Online abuse and other associated risks. Access levels to ICT reflect the curriculum requirements and age of pupils. Staff should guide pupils to online activities that will support the learning outcomes planned for the pupils' age and maturity. This teaching is built into existing lessons alongside our wider whole-school approach including visits from external visitors and assemblies with a running theme of keeping safe. Pupils will explicitly be taught the following topics through their lessons:

- What Internet use is acceptable and what is not and given clear guidelines for Internet use;
- How to use a wide range of devices and learn about their advantages and disadvantages, in different applications;
- How to evaluate what they see online; How to recognise techniques used for persuasion; Online behaviour;
- How to identify online risks and How and when to seek support.
- How to recognise and respond to harmful online challenges and online hoaxes.

We recognise that Peer-on-Peer abuse can occur online and to this end we teach pupils how to spot early warning signs of potential abuse, and what to do if pupils are subject to sexual harassment online. When accessing the Internet individuals are especially vulnerable to a number of risks which may be physically and emotionally harmful, including:

- Access to illegal, harmful or inappropriate images
- Cyber bullying Access to, or loss of, personal information
- Access to unsuitable online videos or games
- Loss of personal images
- Inappropriate communication with others
- Illegal downloading of files
- Exposure to explicit or harmful content, eg involving radicalisation
- Plagiarism and copyright infringement

- Sharing the personal information of others without the individual's consent or knowledge

Online Safety education is reinforced throughout the year alongside our PSHEE programme, These key messages and resources are shared with parents to discuss at home as well. We recognise a one size fits all approach may not be appropriate, and a more personalised or contextualised approach for more vulnerable children e.g., victims of abuse and SEND, is used as appropriate. Staff should be vigilant in lessons where pupils use the Internet. If staff allow the use of mobile devices in their lessons, they must ensure that they are used in line with school policy.

Harmful online challenges and online hoaxes: (Please refer to the latest DfE Guidance) There has been a growing trend in the number of both challenges and hoaxes online as well as their popularity. As such, the school has put in a number of measures to safeguard our children. A hoax is a deliberate lie designed to seem truthful, and online challenges generally involve users recording themselves taking a challenge, and then distributing the video through social media channels, inspiring or daring others to repeat the challenge. We teach pupils to recognise the signs that something may be untruthful online or that risks associated with any online challenges as well as who they can speak to if they have a concern. Where a child or member of staff reports an online hoax or challenge, we ensure that they are taken seriously, and acted upon appropriately, with the best interests of the child coming first. We ensure we provide opportunities to discuss this topic within Online Safety lessons, ensuring children and young people can ask questions and share concerns about what they experience online without being made to feel foolish or blamed.

A case-by-case assessment, establishing the scale and nature of the possible risk to our students will be carried out, and appropriate actions taken, which may include sharing information with parents and carers, our own young people as well as other local schools. Forward planning, together with case-by-case research, will allow for a calm and measured response and avoid creating panic or confusion by spreading information which itself is untrue or would only draw students' attention to a potential risk.

Our DSL will check the factual basis of any harmful online challenge or online hoax with a known, reliable and trustworthy source, such as the Professional Online Safety Helpline from the UK Safer Internet Centre. Where harmful online challenges or online hoaxes appear to be local (rather than large scale national ones) local safeguarding advice, such as from the local authority or local police force, may also be appropriate and helpful. Information that is shared with parents and carers will include encouraging them to focus on positive and empowering online behaviours with their children, such as critical thinking, how and where to report concerns about harmful content and how to block content and users.

Pupils' Use of IT Systems: All pupils must agree to the IT Acceptable Use Policy before accessing the school systems. Pupils at The Roche School will be given supervised access to our computing resources and will be provided with access to filtered Internet and other services operating at the school. Problems with ICT equipment should be reported either to the class teacher or the IT Manager. The promotion of online safety within Computing activities is to be considered essential for meeting the learning and development needs of pupils and young people. The school will ensure that the use of Internet-derived materials by staff and pupils complies with copyright law. The Roche School will help pupils to understand the risks posed by adults or young people, who use the Internet and social media to bully, groom, abuse or radicalise other people, especially pupils, young people and vulnerable adults. Internet safety is integral to the school's Computing curriculum and is also be embedded in our Personal, Social, Health and Economic Education (PSHEE) and Spiritual, Moral, Social and Cultural (SMSC) Development. The latest resources promoted by the DfE can be found at:

- Education for a connected world
- The UK Safer Internet Centre (www.saferinternet.org.uk)
- CEOP's Thinkuknow website (www.thinkuknow.co.uk)
- Teaching Online Safety in School https://www.gov.uk/government/publications/teaching-online-safety-in-schools
- Google Legends (KS2) (https://beinternetlegends.withgoogle.com/en_uk)

Educating Staff: Staff and the Advisory Board will be provided with sufficient online safety training to protect pupils and themselves from online risks and to deal appropriately with Online Safety incidents when they occur. Ongoing staff development

training includes training in online safety, together with specific safeguarding issues including cyberbullying and radicalisation. The frequency, level and focus of such training will depend on individual roles and requirements. Staff will undergo online safety training annually/when changes occur basis to ensure they are aware of current online safety issues and any changes to the provision of online safety, as well as current developments in social media and the Internet as a whole. All staff will employ methods of good practice and act as role models for young people when using the Internet and other digital devices. All staff will be educated on which sites are deemed appropriate and inappropriate. All staff are reminded of the importance of acknowledging information they access online, in order to avoid copyright infringement and/or plagiarism. Any new staff are required to undergo online safety training as part of their induction programme, ensuring they fully understand this online safety policy/social media policy/user agreement. The Online Safety Officer will act as the first point of contact for staff requiring online safety advice.

Communicating and Educating parents/carers in online safety: We believe that it is essential for parents/carers to be fully involved with promoting online safety both in and outside of school and to be aware of their responsibilities. We regularly consult and discuss online safety with parents/carers and seek to promote a wide understanding of the benefits of new technologies, together with the associated risks. For example, parents/carers are required to make a decision as to whether they consent to images of their child being taken and used in the public domain (e.g., on School website). The Roche School recognises the crucial role that parents/carers play in the protection of their children with regards to online safety. The school organises an annual awareness session for parents/carers with regards to online safety which looks at emerging technologies and the latest ways to safeguard pupils from inappropriate content. The school will also provide parents/carers with information through newsletters, and the school parent app. Parents/carers are always welcome to discuss their concerns on online safety with the school, who can direct them to the support of our Online Safety Officer if required. Parents/carers will be encouraged to support the school in promoting good online safety practice.

Protecting Personal Data: Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018 and the UK General Data Protection Regulations (GDPR) 2020. The school recognises that if required, data may need to be obtained by relevant parties such as the Police. Pupils are encouraged to keep their personal data private as part of our online safety lessons and Computing curriculum, including areas such as password protection and knowledge about apps and unsecured networks/apps etc. The school will be responsible for ensuring there is an appropriate level of security procedures in place, in order to safeguard systems, staff and learners and will review the effectiveness of these procedures periodically to keep up with evolving cyber-crime technologies.

Radicalisation and the Use of Social Media to Encourage Extremism: The Internet and the use of social media in particular has become a major way to communicate with others, especially young people, which has provided access for like-minded people to create an online community and promote extreme beliefs, sharing extreme ideological views or advocating the use of violence to solve problems. This has led to social media becoming a platform for:

- intensifying and accelerating the radicalisation of young people; promoting extreme beliefs;
- accessing likeminded people where they are not able to do this off-line, creating an online community;
- normalising abnormal views and behaviours, such as extreme ideological views or the use of violence to solve problems and address grievances.

The Roche School has a number of measures in place to help prevent the use of social media for this purpose:

- Website filtering is in place to help prevent access to terrorist and extremist material and social networking sites such as Facebook, Instagram or Twitter by pupils.
- Pupils, parents/carers and staff are educated in safe use of social media and the risks posed by online activity, including from extremist and terrorist groups.

Further details on how social media is used to promote extremism and radicalisation can be found in guidance from the Department for Education '*How Social Media Is Used to Encourage Travel to Syria and Iraq: Briefing Note for Schools.'*

Filtering and Monitoring: The school provides a safe environment for students to learn and work in, especially when online.

Filtering and monitoring are both important parts of safeguarding students from potentially harmful and inappropriate online material. The proprietor has overall strategic responsibility for filtering and monitoring. For this to occur, they have assigned a member of senior leadership team (The DSL) and the Chair of the School's Advisory Board is responsible for ensuring these standards are met. The Senior DSL works closely with the IT Manager, Computing Co-ordinator and other members of SLT to ensure that filtering and monitoring is adequate and robust in the school. The school considers those who are potentially at greater risk of harm and how often they access the school's IT systems. The school follows the Filtering and Monitoring Standards (DfE: 2023) which ensures that the school:

- identifies and assigns roles and responsibilities to manage filtering and monitoring systems;
- reviews filtering and monitoring provision at least annually;
- blocks harmful and inappropriate content without unreasonably impacting teaching and learning.
- has effective monitoring strategies in place that meet the school's safeguarding needs

The IT Team and Senior DSL have ensured:
The filtering provider MUST be a member of Internet Watch Foundation (IWF), signed up to Counter-Terrorism Internet Referral Unit list (CTIRU) and block access to illegal content including child sexual abuse material (CSAM).

- Any specific risks or vulnerable pupil groups are identified (age of students, SEND issues, EAL, PSHE, RSE, County Lines, BYOD etc.)
- All existing school computers and devices are monitored and checked by the IT Manager.

Technology and Prevent Duty: As part of an integrated policy linked to the Prevent strategy, the School also has a duty to ensure that students are prevented and protected from the risk of being radicalised through the access to extremistpropaganda, e.g. from ISIL. The School must promote British values through the curriculum and SMSC and SRE. Teachers must also be aware of their responsibility to monitor and report any serious concerns they have about a student's use or access to inappropriate material, especially that which undermines British values and tolerance of others. The School's network and facilities must NOT be used for the following activities:

- Accessing or downloading pornographic material;
- Gambling
- Accessing sites or social media channels that promote extreme viewpoints and radical propaganda
- Soliciting for personal gain/profit
- Revealing or sharing proprietary or confidential material
- Representing personal opinions about the School;
- Positing indecent or humiliating images or remarks/proposals

Assessing Risks Online: We will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the School network. The School cannot accept liability for any material accessed, or any consequences of Internet access.

Developing technologies, such as mobile phones with Internet access are not governed by the School's infrastructure and can bypass any and all security and filtering measures that are or could be deployed. To address this, the School works with students across our age range to ensure that students are educated clearly about the risks of both social media and internet use, alongside regular monitoring of device usage as appropriate.

- We will audit IT use to establish if the Online Safety policy is sufficiently robust and that the implementation of the Online Safety policy is appropriate and effective.
- Methods to identify, assess and minimise risks will be reviewed regularly.
- The Advisory Board will review and examine emerging technologies for educational benefit and a risk assessment will be carried out before use in School is allowed.
- Any person not directly employed by the School will not be provided with access to any of the School systems with the exception of filtered *Wi-Fi* access.

- The Roche School takes measures to ensure appropriate IT filters monitoring systems are in place to safeguard students from potentially harmful and inappropriate material on-line without unreasonable "over-blocking"
- Year 6 children only may bring their mobile device to school and must hand it in to the office or their class teacher at the beginning of the day, returned at the end of the day. The School recognises that students may choose to circumvent certain safety precautions by using mobile data on their devices over 3G, 4G and 5G. To help provide a safe environment for all students, we will supplement the systems filtering with behaviour management and additional staff/student training.

Cyber Security: The school recognises its responsibility to ensure that appropriate security protection procedures are in place to safeguard our systems. As part of our whole-school Online Safety Training, we ensure staff, advisory board and proprietor are updated with the evolving cyber-crime technologies. In addition, the school activity considers the Cyber security standards (DfE: 2023) and uses these as a base for keeping the school and its community safe from cyber-crime**.**

Phishing and Pharming Definition: A phishing email usually contains a link with directions asking the recipient to click on it. Clicking the link transports the email recipient to an authentic looking, albeit fake, web page. The target is asked to input information like a username and password, or even additional financial or personal data.
The miscreant that orchestrates the phishing scheme is able to capture this information and use it to further criminal activity, like theft from a financial account and similar types of criminal activity.
The School has no intention of changing its financial information, therefore never accept an email with a link pretending to be the School's accounts department.
Top tips:

- Never click on hyperlinks in email from an unknown sender, rather manually type the URL into the web browser itself
- Never enter sensitive information in a pop-up window except at those sites that an individual knows to be trustworthy
- Verify HTTPS on the address bar - whenever a person is conveying confidential information online, you must confirm that the address bar reads "HTTPS" and not the standard "HTTP." The "S"confirms that the date is being conveyed through a legitimate, secured channel
- Access personal and financial information only from a computer or device you trust to be free from trojans and keyloggers
- Education on phishing and pharming attacks - staying abreast of phishing scams and the technology and techniques designed to prevent them is crucial. A plethora of reliable educational resources exist on the Internet that are designed to assist a person in preventing phishing attacks
- Report phishing and pharming to the financial institution, the FTC, and the Internet Crime Complaint Center

Characteristics of a strong password

- At least 8 characters – the more characters, the better
- A mixture of both uppercase and lowercase letters
- A mixture of letters and numbers
- Inclusion of at least one special character, e.g., ! @ # ?]

Note: do not use < or > in your password, as both can cause problems in web browsers
A strong password is hard to guess, but it should be easy for you to remember – a password that has to be written down is not strong, no matter how many of the above characteristics are employed.

Protecting Personal Data: Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018 and the General Data Protection Regulations (GDPR) 2018. The School recognises that if required, data may need to be obtained by relevant parties such as the Police. Students are encouraged to keep their personal data private as part of our Online Safety lessons and Computing curriculum, including areas such as password protection and knowledge about apps and unsecured networks/apps etc. The School will act responsibly to ensure we have an appropriate level of security protection procedures in place, in order to safeguard systems, staff and learners and we review the effectiveness of these procedures periodically to keep up with evolving cyber-crime technologies.

Acceptable use of the internet in the School: All students, parents, staff, volunteers and proprietors are expected to sign an agreement regarding the acceptable use of the School's IT systems and the internet (appendices 1 and 2). Visitors will be expected to read and agree to the School's terms on acceptable use if relevant. Use of the School's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role. We will monitor the websites visited by students, staff, volunteers, proprietors and visitors (where relevant) to ensure they comply with the above.
More information is set out in the **acceptable use agreements** in appendices 1 and 2.

Reporting of Online Safety Issues and Concerns Including Concerns Regarding Radicalisation: The Roche School has clear reporting mechanisms in place, available for all users to report issues and concerns. For staff, any concerns regarding online safety should be made to the Online Safety Officer, who will review the issue and take the appropriate action. For pupils, they are taught to raise any concerns to their class teacher who will then pass this on to the Online Safety Officer. Complaints of a child protection nature must be dealt with in accordance with our Safeguarding & Child Protection Policy.

Our Designated Safeguarding Lead (DSL) provides advice and support to other members of staff on protecting pupils from the risk of online radicalisation. The Roche School ensures staff understand what radicalisation and extremism mean and why people may be vulnerable to being drawn into terrorism. We ensure staff have the knowledge and confidence to identify pupils at risk of being drawn into terrorism, and to challenge extremist ideas, which can be used to legitimise terrorism. Staff safeguard and promote the welfare of pupils and know to report any concerns to the DSL.

Assessing Risks:

- We will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school network. The school cannot accept liability for any material accessed, or any consequences of Internet access.
- Developing technologies, such as mobile phones with Internet access are not governed by the school's infrastructure and can bypass any and all security and filtering measures that are or could be deployed. We recognise the additional risks this has for our pupils, who could have unsupervised access to the Internet when using their own devices. To address this, the school works with pupils across our age range to ensure that pupils are educated clearly about the risks of both social media and Internet use, alongside regularly monitoring of device usage as appropriate.
- We will audit ICT use to establish if the Online Safety policy is sufficiently robust and that the implementation of the Online Safety policy is appropriate and effective.
- Methods to identify, assess and minimise risks will be reviewed regularly.
- The Advisory Board will review and examine emerging technologies for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Any person not directly employed by the school will not be provided with access to any of the school systems with the exception of filtered *Wi-Fi* access, if necessary.
- The Roche School takes measures to ensure appropriate IT filters monitoring systems are in place to safeguard pupils from potentially harmful and inappropriate material on-line without unreasonable "over-blocking"
- The school recognises that students may choose to circumvent certain safety precautions by using mobile data on their devices over 3G, 4G and 5G. To help provide a safe environment for all students, we will supplement the systems filtering with behaviour management and additional staff/student training. Pupils must place any personal mobile devices in the school office or with their class teacher when arriving at school and may collect them on their way out at the end of the day.

Mobile Electronic Devices (Phones, Laptops, iPads and Tablets; please see appendix 3 for more details): Smart Mobile telephones and smart watches are not permitted to be brought to school by pupils . Year 6 pupils may bring in 'brick' mobile phones without internet connectivity but must leave their mobile devices in the school office or with class teacher upon arrival, and collect them at the end of the school day. Mobile phones are kept on site at the risk of the individual pupil. The Roche School is not responsible for any devices lost or damaged whilst on school grounds.

Recordings made using mobile electronic devices: Using the camera on a phone or similar device, either to photograph/film/record any member of the school community, do any form of live streaming or to show to others the photos/videos/audio recordings already on the phone or similar device is prohibited. The discovery of any uploads to social media platforms will result in serious sanctions being applied.

Cyber-Bullying: Cyber-Bullying is the use of ICT, particularly mobile electronic devices and the Internet, deliberately to upset someone else. Cyberbullying (along with all forms of bullying) will not be tolerated and incidents of cyberbullying should be reported and will be dealt with in accordance with the school's Anti-Bullying Policy.

Online Sexual Harassment: Sexual harassment creates an atmosphere that, if not challenged, can normalise inappropriate behaviours and provide an environment that may lead to sexual violence. online sexual harassment include: non-consensual sharing of sexual images and videos and sharing sexual images and videos (both often referred to as sexting); inappropriate sexual comments on social media; exploitation; coercion and threats. Online sexual harassment may be standalone, or part of a wider pattern of sexual harassment and/or sexual violence. All cases or allegations of sexual harassment, online or offline, is unacceptable and will dealt with under our Child Protection Procedures. (Please see our Safeguarding – Child Protection Policy for more details)

Additionally, we recognise that incidents of sexual violence and sexual harassment that occur online (either in isolation or in connection to offline incidents) can introduce a number of complex factors. These include the potential for the incident to take place across a number of social media platforms and services and for things to move from platform to platform online. It also includes the potential for the impact of the incident to extend further than the school's local community (e.g. for images or content to be shared around neighbouring schools/colleges) and for a victim (or alleged perpetrator) to become marginalised and excluded by both online and offline communities. There is also the strong potential for repeat victimisation in the future if abusive content continues to exist somewhere online. Online concerns can be especially complicated. Support is available at:

a. The UK Safer Internet Centre provides an online safety helpline for professionals at 0344 381 4772 and helpline@saferInternet.org.uk. Providing expert advice and support for school staff with regard to online safety issues and when an allegation is received.
b. If the incident involves sexual images or videos that have been made and circulated online, we will support the victim to get the images removed through the Internet Watch Foundation (IWF). The IWF will make an assessment of whether the image is illegal in line with UK Law. If the image is assessed to be illegal, it will be removed and added to the IWF's Image Hash list.

Online Forms of Abuse (Also see our Safeguarding Child Protection Policy): Information and communication technology (ICT)-based forms of child physical, sexual and emotional abuse can include bullying via mobile telephones or online (internet) with verbal and visual messages. This can also include child sexual abuse. All staff are alert to the signs that a child may be at risk of may have been abused online and will follow the school's child protection procedures (Please see our Child Protection Policy for more details).

ICT-Based Sexual Abuse (Including Sexting): The impact on a child of ICT-based sexual abuse is similar to that for all sexually abused pupils. However, it has an additional dimension in that there is a visual record of the abuse. ICT-based sexual abuse of a child constitutes significant harm through sexual and emotional abuse. Recognition and response is recognising a situation where a child is suffering, or is likely to suffer a degree of physical, sexual and/or emotional harm (through abuse or neglect) which is so harmful that there needs to be compulsory intervention by child protection agencies into the life of the child and their family. All adults (volunteers, staff) working with pupils, adults and families will be alerted to the possibility that:

- A child may already have been/is being abused and the images distributed on the Internet or by mobile telephone;
- An adult or older child may be grooming a child for sexual abuse, including involvement in making abusive images. This process can involve the child being shown abusive images;
- An adult or older child may be viewing and downloading child sexual abuse images.

Older pupils are reminded that 'sexting' (sending or posting images or videos of a sexual or indecent nature) is strictly prohibited by the school and may constitute a criminal offence. The school will treat incidences of sexting (both sending and receiving) as a

safeguarding issue and pupils concerned about images that they have received, sent or forwarded should speak to any member of staff for advice.

There are no circumstances that will justify adults possessing indecent images of pupils. Adults who access and possess links to such websites will be viewed as a significant and potential threat to pupils. Accessing, making and storing indecent images of pupils is illegal. This will lead to criminal investigation and the individual being barred from working with pupils, if proven. Adults should not use equipment belonging to the school to access adult pornography; neither should personal equipment containing these images or links to them be brought into the workplace. This will raise serious concerns about the suitability of the adult to continue to work with pupils. Adults should ensure that pupils are not exposed to any inappropriate images or web links. Where indecent images of pupils or other unsuitable material are found, the police and Local Authority Designated Officer (LADO) should be immediately informed. Adults should not attempt to investigate the matter or evaluate the material themselves, as this may lead to evidence being contaminated, which in itself can lead to a criminal prosecution.

Sanctions: Sanctions will depend on the severity of the offence as assessed by the Senior Leadership Team. They may include one or more of the following:

- Temporary or permanent ban on the use of ICT resources in the School.
- Temporary or permanent ban on the use of the Internet in the School.
- Additional disciplinary action may be added in line with existing practice on inappropriate language or behaviour.
- Temporary or permanent exclusion from school may be imposed.
- If appropriate, police or local authorities may be involved.

The Child Exploitation and Online Protection (CEOP) Tel: 0370 496 7622 Email: communication@nca.x.gsi.gov.uk brings together law enforcement officers, specialists from children's charities and industry to tackle online child sexual abuse. CEOP provides a dedicated 24 hour online facility for reporting instances of online child sexual abuse. The main concern for teachers is the safe and effective supervision of pupils using the internet in school. The CEOP website is an invaluable source of information and resources concerned with e-safety. However, many pupils now use the internet at home for homework and socialising, therefore the staff will need to help the parents understand the positive ways in which the internet can be used but also some of the associated risks. The website www.becta.org.uk outlines clearly the requirements of a school to control the pupil's internet viewing and instate 'Acceptable Use Policies'.

Chat Room Grooming and Offline Abuse: Our staff need to be continually alert to any suspicious activity involving computers and the Internet. Grooming of pupils online is a faster process than usual grooming, and totally anonymous. The abuser develops a 'special' relationship with the child online (often adopting a false identity), which remains a secret to enable an offline meeting to occur in order for the abuser to harm the child.

Social Media, including Facebook, Twitter and Instagram: Facebook, Twitter, Instagram and other forms of social media are increasingly becoming an important part of our daily lives, including part of the school's marketing strategy.

- Staff are not permitted to access their personal social media accounts using school equipment at any time, unless granted prior permission by the Headteacher for reasons of work
- Staff are advised not to befriend or follow parents/carers of pupils and to keep their personal profile as private as possible
- Staff and pupils are provided with information on how to use social media responsibly and what to do if they are aware of inappropriate use by others
- Staff and pupils, are aware that the information, comments, images and video they post online can be viewed by others, copied and stay online forever

Staff and pupils are aware that their online behaviour should at all times be compatible with UK law. Additionally, more information on best practice for staff can be found in our Staff Behaviour (Code of Conduct) Policy.

The Roche School recognises that Social media is very likely to play a central role in the fall out from any incident or alleged incident. There is the potential for contact between victim and alleged perpetrator and a very high likelihood that friends from either side could well harass the victim or alleged perpetrator online.

Taking and Storing Images of Pupils Including Mobile Phones (See our related documents including Appendix 4): The Roche School provides an environment in which pupils, parents/carers and staff are safe from images being recorded and inappropriately used. Upon their initial visit, parents/carers, volunteers and visitors are given information informing them they are not permitted to use mobile phones on the premises in the presence of pupils, or to take photographs of pupils apart from circumstances as outlined in Appendix 6 of this policy. This prevents staff from being distracted from their work with pupils and ensures the safeguarding of pupils from inappropriate use of mobile phone cameras and other digital recording equipment. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images of themselves and others especially on social networking sites.
- Photographs published onto any website will comply with good practice guidance on the use of such images. Care will be taken to ensure that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute. Their full names will not be used anywhere in the website, particularly in association with photographs.

N.B. The word 'camera' in this document refers to any device that may be used to take and store a digital image e.g. mobile phone, tablet, laptop etc. The school has an Electronic Devices Acceptable Use Policy which includes:

- The commitment to keep the pupils safe.
- How we manage the use of mobile phones and smart watches at The Roche School, taking into consideration staff, volunteers, other professionals, visitors and parents/carers.
- How we inform parents/carers, visitors and other professionals of our procedures.
- What type of mobile phones will be used on educational visits and learning outside the classroom.
- The consequences of any breaches of this policy.
- Reference to other policies, such as Whistleblowing and Safeguarding Children-Child Protection Policies.

Remote Learning (Please see our Remote Learning Policy for more details): Where there are periods in which the school is forced to close, yet continue to provide education (such as during the COVID-19 Pandemic) it is important that The Roche School supports staff, pupils and parents/carers to access learning safely, especially considering the safety of our vulnerable pupils. Staff and volunteers are aware that this difficult time potentially puts all children at greater risk and the school recognises the importance of all staff who interact with children, including online, continuing to look out for signs a child may be at risk. Staff and volunteers will continue to be alert to any signs of abuse, or effects on learners' mental health that are also safeguarding concerns, and will act on concerns immediately. Any such concerns should be dealt with as per the Child Protection Policy and where appropriate referrals should still be made to children's social care and as required, the police. Online teaching should follow the same principles as set out in the school's staff and pupils' respective Behaviour - Code of Conducts. Additionally, school name will ensure any use of online learning tools and systems is in line with privacy and data protection/GDPR requirements.

The school will put additional measures in place to support parents and students who are learning from home. This will include specific guidance on which programmes the school is expecting students to use and how to access these alongside how students and parents can report any concerns that they may have. Guidance will also be issued on which staff members students will have contact with and how this will happen, including how to conduct virtual lessons (including video conferencing). Details of this can be found in our schools Remote Learning Policy.

Additionally, the Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, with the day-to-day responsibility being delegated to the Online Safety Officer who is our DSL. The Headteacher is aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff, which in line with our main safeguarding reporting procedures.

Staff working remotely should wherever possible use their school-issued ICT equipment, however they may use their own computer equipment if this is not practical, as long as it is in accordance with the school's Data Protection Policy. Staff are responsible for security of personal data and must ensure it is stored securely when using personal systems or remote systems to maintain confidentiality from other members of the household.

Artificial Intelligence (AI) use in school

Here at The Roche School we understand the valuable potential that artificial intelligence (AI), including generative AI, holds for schools. For example, it can be used to enhance pedagogical methods, customise learning experiences and progress educational innovation.

We are also aware of the risks posed by AI, including data protection breaches, copyright issues, ethical complications, safeguarding and compliance with wider legal obligations.

Please see our 'Use of Artificial Intelligence (AI)' Policy for further information.

Related documents:

- Safeguarding Children- Child Protection Policy; Sexual Violence and Sexual Harassment (Including Peer-on-Peer Abuse Policy); Anti-Bullying Policy; Behaviour Management Policy; Staff Behaviour (Code of Conduct), Use of Artificial Intelligence Policy.
- Prevent Duty: Tackling Extremism and Radicalisation Policy; Spiritual, Moral, Social and Cultural Development (SMSC); Personal; Personal Social, Health, Economic Education (PSHEE)