Founded 1125

Policy number E35

Reading School

Online Safety Policy

Responsibilities
Policy Owner: Gareth Sellwood
Network Manager
Governors Committee EXPC

Audit Control
Policy created: 04/10/2021
Date of next review Nov 2026
Version: 1.0
Statutory policy Yes

Online Safety Policy

Document Control and Approval

Version Control

Version	Author	Summary of Changes	Reviewed By	Date
1.0	Jonathan Hitchinson	Policy created	Jonathan Hitchinson	11/05/2021
	Govs Clerk	Review date changed to 2023	EXPC Cttee	3/10/2022
2.0	**Lizzie Ayres**	**Policy developed and amended. Externally reviewed**		**23/9/23**
		Approved	EXPC Committee	02/10/2023
		Reviewed	EX{C Committee	30/09/2024
2.1	Lizzie Ayres	Updated for KCSIE 2025		

Responsibilities

Job title	Responsible for;
Network Manager	Policy Owner
Chief Operating Officer	Policy Overview
EXPC	Committee Responsible

Policies Linked

Policy name
Mobile phone policy
Safeguarding and child protection
Behaviour policy
Staff disciplinary policy
Data protection policy and privacy notices
Complaints policy

Online Safety Policy

Contents

Online Safety Policy

Policy Aims and Statement

E-safety may be described as the school's ability to protect and educate pupils and staff in their use of technology and to have the mechanisms in place to intervene and support any incident where appropriate.

Reading School aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Identify and support groups of pupils that are potentially at greater risk of harm online than others
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as 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, such as 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

Safeguarding is a serious matter; at Reading School we use technology and the Internet extensively across all areas of the curriculum. Online safeguarding, known as E-Safety, is an area that is constantly evolving and as such this policy will be reviewed on an annual basis or in response to an E-safety incident, whichever is sooner.

The purpose of this policy is two-fold:

1. To ensure the requirement to empower the whole school community with the knowledge to stay safe and risk free is met.
2. To ensure risks are identified, assessed and mitigated (where possible) in order

to reduce any foreseeability of harm to the student or liability to the school.

This policy is available for anybody to read on the Reading School website. All members of staff will sign as read and understood this e-safety policy, the Staff Social Media Policy and the Staff Acceptable Use Policy. Every student must sign the ICT usage agreement before gaining access to the computer network systems. This policy is part of that agreement.

Legislation and Guidance

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

Policy Governance (Roles & Responsibilities)

Governing Body

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation. The governing board will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring. The governing board will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governing board should ensure children are taught how to keep themselves and others safe, including keeping safe online. The governing board must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The boardwill review the DfE filtering and monitoring standards, and discuss with IT staff and

service providers what needs to be done to support the school in meeting thosestandards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
- Reviewing filtering and monitoring provisions at least annually;
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;
- Having effective monitoring strategies in place that meet their safeguarding needs.

All governors will:

- Ensure they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 3)
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole-school or college approach to safeguarding and related policies and/or procedures
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

Individual governors will abide by the guidance for school governors on online social networking produced by the National Co-ordinators of Governor Serviceshttp://www.ncogs.org.uk/(NCOGS), set out in Appendix 6.

Headmaster

Reporting to the governing body, the Headmaster has overall responsibility for online safety within the school. The day-to-day management of this will be delegated to a member of staff, the online Safety Officer (or more than one), as indicated below.

The Headmaster will ensure that:

- E-Safety training throughout the school is planned and up to date and appropriate to the recipient, i.e. students, all staff, senior leadership team and governing body, parents.
- The designated e-Safety Officer(s) has had appropriate CPD in order to undertake the day to day duties.
- All e-safety incidents are dealt with promptly and appropriately.

Designated Safeguarding Lead

Details of the school's designated safeguarding lead (DSL) and deputies duties are set out in our Safeguarding and Child Protectionpolicy, as well as relevant job

descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher and governing board to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly
- Providing governors with assurance that filtering and monitoring systems are working effectively and reviewed regularly
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Working with the ICT manager to make sure the appropriate systems and processes are in place
- Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school's child protection policy
- Ensuring that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety (appendix 4 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing board
- Undertaking annual risk assessments that consider and reflect the risks children face
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

This list is not intended to be exhaustive.

The Network Manager

The network manager will:

- Put in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material

- Ensure that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conduct a full security check and monitoring the school's ICT systems on a fortnightly basis
- Block access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Keep up to date with the latest risks to children whilst using technology; familiarise themselves with the latest research and available resources for school and home use.
- Review this policy regularly and bring any matters to the attention of the Headmaster.
- Advise the Headmaster and governing body on all e-safety matters.
- Engage with parents and the school community on e-safety matters at school and/or at home.
- Liaise with IT technical support and other agencies as required.
- Retain overall responsibility for e-safety incident reporting, ensuring that any are logged and dealt with appropriately in line with this policy
- Ensure that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Ensure any technical e-safety measures in school (e.g. Internet filtering software, behaviour management software) are fit for purpose.
- Make him/herself aware of any reporting function with technical e-safety measures, i.e. internet filtering reporting function; liaise with the Headmaster and responsible governor to decide on what reports may be appropriate for viewing.

IT Technical Support Staff

Technical support staff are responsible for ensuring that the IT technical infrastructure is secure; this will include at a minimum:

- Anti-virus is fit-for-purpose, up to date and applied to all capable devices. Software updates are regularly monitored and devices updated as appropriate. Any e-safety technical solutions such as Internet filtering are operating correctly.
- Filtering levels are applied appropriately and according to the age of the user; that categories of use are discussed and agreed with the e-safety officer and Headmaster.
- Passwords are applied correctly to all users. Passwords for staff will be a minimum of 8 characters with uppercase and numbers.
- The IT System has a secure password and access policy.

Teaching and Associate Staff

All staff, including contractors and agency staff, and volunteers are responsible for:

- Engaging with, understanding and maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT

systems and the internet, and ensuring that pupils follow the school's terms on acceptable use.

- Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing by informing the IT manager.
- Following the correct procedures by speaking with the IT manager if they need to bypass the filtering and monitoring systems for educational purposes
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'
- All details within this policy are understood. If anything is not understood it should be brought to the attention of the Headmaster.

All Students

The boundaries of use of ICT equipment and services in this school are given in the student Acceptable Use Policy
Any deviation or misuse of ICT equipment or services will be dealt with in accordance with the behaviour policy.
E-Safety is embedded into the curriculum - students will be given the appropriate advice and guidance by staff, in all subject areas across the curriculum.
All students will be fully aware how they can report areas of concern whilst at school or outside of school.

Parents and Carers

Parents play the most important role in the development of their children; as such the school will ensure that parents have access to resources to acquire the skills and knowledge they need to ensure the safety of children outside the school environment. Through parents' evenings, school newsletters and the availability of free online training courses the school will keep parents up to date with new and emerging e-safety risks, and will involve parents in strategies to ensure that students are empowered.

Parents must also understand the school needs have to rules in place to ensure that their child can be properly safeguarded. As such all new Year7 parents will sign the student Acceptable Use Policy before their child can be granted any access to school network, ICT equipment or services.

Parents/carers are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy

- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet

Parents/carers can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? –UK Safer Internet Centre
- Hot topics –Childnet International
- Parent resource sheet –Childnet International
- Child Exploitation and Online Protection Command - CEOP Safety Centre

Visitors and Members of the Community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use

Network and Device Management

Reading School uses a range of devices including PC's, laptops and tablets. In order to safeguard the student and in order to prevent loss of personal data we employ the following assistive technology:

Internet Filtering

We use a Smoothwallweb filter that prevents unauthorised access to illegal websites, including those sites deemed inappropriate under the Prevent Agenda. It also prevents access to inappropriate websites; appropriate and inappropriate is determined by the age of the user and will be reviewed in line with this policy or in response to an incident, whichever is sooner. The E-Safety Officer, DSL and IT Support are responsible for ensuring that the filtering is appropriate and that any issues are brought to the attention of the Headmaster. Web access is logged indefinitely for all users of the ICT systems in Reading School.

Email Filtering

We use forefront Office 365 technology that prevents any infected email to be sent from the school, or to be received by the school. Infected is defined as: an email that contains a virus or script (i.e. malware) that could be damaging or destructive to data; spam email such as a phishing message. The system is also used to filter certain words and can be used for monitoring.

Passwords

All staff and students will be unable to access the network without a unique username and password.Staff and student passwords should be changed if there is a suspicion that it has been compromised.The network Manager will be responsible for ensuring that passwords are changed as and when required. The use of another

person's credentials at any time, is forbidden.

Anti-Virus

All capable devices will have anti-virus software. This software will be updated at least weekly for new virus definitions. IT Support will be responsible for ensuring this task is carried out, and will report to the Headmaster if there are any concerns.

Education – Informing about Online Safety

Students

Ensuring that students are safe when working online, either in class or at home, is a priority for all staff at Reading School, both teaching and associate staff. This is to be achieved not by "locking down" access to the internet but by making students aware of the risks the web may contain so that they can make informed judgements for their own safety, for themselves.

Pupils will be taught about online safety as part of the curriculum:

All schools have to teachRelationships and sex education (RSE) and health education.

In **Key Stage 3**, pupils will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report a range of concerns

Pupils in **Key Stage 4** will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns

By the **end of secondary school**, pupils will know:

- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online
- The characteristics of social media, including that some social media accounts are fake, and / or may post things which aren't real / have been created with AI. That social media users may say things in more extreme ways than they might in face-to-face situations, and that some users present highly exaggerated or idealised profiles of themselves online
- Not to provide material to others that they would not want shared further and not to share personal material which is sent to them
- What to do and where to get support to report material or manage issues online

- About the prevalence of deepfakes including videos and photos, how deepfakes can be used maliciously as well as for entertainment, the harms that can be caused by deepfakes and how to identify them
- That the internet contains inappropriate and upsetting content, some of which is illegal, including unacceptable content that encourages misogyny, violence or use of weapons. Pupils should be taught where to go for advice and support about something they have seen online. Pupils should understand that online content can present a distorted picture of the world and normalise or glamorise behaviours which are unhealthy and wrong
- The impact of viewing harmful content
- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence that carries severe penalties including jail
- How information and data is generated, collected, shared and used online
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours
- How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online)
- That social media can lead to escalations in conflicts, how to avoid these escalations and where to go for help and advice
- How to identify when technology and social media is used as part of bullying, harassment, stalking, coercive and controlling behaviour, and other forms of abusive and/or illegal behaviour and how to seek support about concerns
- That websites may share personal data about their users, and information collected on their internet use, for commercial purposes (e.g. to enable targeted advertising)
- That criminals can operate online scams, for example using fake websites or emails to extort money or valuable personal information. This information can be used to the detriment of the person or wider society. About risks of sextortion, how to identify online scams relating to sex, and how to seek support if they have been scammed or involved in sextortion
- That AI chatbots are an example of how AI is rapidly developing, and that these can pose risks by creating fake intimacy or offering harmful advice. It is important to be able to critically think about new types of technology as they appear online and how they might pose a risk
- Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

- The safe use of social media and the internet will also be covered in other subjects where relevant.

Parents

The school will raise parents/carers' awareness of internet safety in communications home, and in information via our website. This policy will also be shared with parents/carers.

Online safety will also be covered during parents' evenings.

The school will let parents/carers know:

- What systems the school uses to filter and monitor online use
- What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online

If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the headteacher.

Safe Use

Acceptable use of the internet in school

All pupils, parents/carers, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet. 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 pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above and restrict access through filtering systems where appropriate.

Use of the school network, with access to the Internet, in school is a privilege, not a right.

Use will be granted to new staff upon signing of this E-safety Policy, staff Social Media Policy (see Appendix 3) and the staff Acceptable Use Policy (see Appendix 2). All students will have access to a copy of this E-safety Policy, the Student Social Media Policy (see Appendix 5) and the student Acceptable Use Policy (see Appendix 4). Access to the network will be granted to new students upon signing and returning their acceptance of the Acceptable Use Policy. ***These policies apply to all staff and students, including Boarding, whether access to the school network or internet is by cable or wireless (or personal mobile account whilst on school premises, including school trips either in the UK or abroad) and on any device, laptop or PC, either school owned or personal.***

In the specific case of Boarding, and at the discretion of the Head of Boarding and on advice from the Network Manager, the internet filters are changed to allow access to certain websites to boarders not available to pupils during the school day, primarily some social networking sites. This is in an attempt to replicate access to those sites non-boarders could reasonably expect at home during the week. Boarding staff have been issued software that allows them to remotely monitor the online activity of individual boarders during the evenings and the usual tracking and reporting logs, as used during the day, still maintain.

Pupils using mobile devices in school

Pupils may bring mobile devices into school, but are not permitted to use them during:

- Lessons
- Lunch or break times
- Tutor group time
- Clubs before or after school, or any other activities organised by the school

Any use of mobile devices in school by pupils must be in line with the acceptable use agreement.

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy.

Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date by always installing the latest updates
- Staff members must not use the device in any way that would violate the school's terms of acceptable use.
- Work devices must be used solely for work activities.
- If staff have any concerns over the security of their device, they must seek advice from the IT Manager.

Email

All staff are reminded that emails are subject to Freedom of Information requests, and as such the email service is expected to be used for professional work-based emails only. The use of personal email addresses for the purposes of contacting students is not permitted.

Students are permitted to use the school email system, and as such will be given their own email address, based on their network user name. Students should use this email account only for school-based activity as laid out in the student Acceptable Use Policy that they have signed on entry to the school. Students are expected to regularly check their email and use formal address when contacting both staff and peers via email. Please refer to the Communications Policy.

Photos and videos

All parents sign a photo release slip on entry to the school, as part of the Induction Pack they receive; non-return of the permission slip will not be assumed as acceptance.

How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, the school will follow the procedures set out in our policies on behaviour and ICT and internet acceptable use. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents that involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

Notice and take down policy

Should it come to the school's attention that there is a resource which has been inadvertently uploaded, either to the school website or school/department authorised social networking sites, and the school does not have copyright permission to use that resource, it will be removed within one working day.

Reporting E-safety Incidents

Any e-safety incident is to be brought to the immediate attention of the e-Safety Officer, or in their absence the Headmaster. The e-Safety Officer will assist in taking the appropriate action to deal with the incident and to fill out an incident log. All staff should make themselves aware of the procedures and the responsible staff involved in this process:

1. School E-Safety Incident
2. Staff member reports to Head of House

3. HOH consults E-Safety Officer, DSL and sends report
4. Evidence Gathering
5. E-Safety Officer and DSL consults SLT on result
6. Incident is logged in safeguarding files

Training and Curriculum

It is important that the wider school community is sufficiently empowered with the knowledge to stay as risk free as possible whilst using digital technology; this includes updated awareness of new and emerging issues. This includes the regular distribution of e-safety information to staff, students and parents.

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues, including cyber-bullying and the risks of online radicalisation.

In addition, Reading School will have an annual programme of online e-safety training for teaching/associate staff, to be incorporated within the CPD programme, with the Board of Governors included. This online e-safety training provides staff with a certificate which must be renewed by further training on an annual basis. This continuous rolling training programme means that staff will always be up to date with the latest issues on e-safety from new and evolving technologies.

The school should ensure that aspects of e-Safety for students is firmly embedded into the curriculum. Whenever ICT is used in the school, staff will ensure that students are made aware about the safe use of technology and risks as part of the student's learning. If asked, Heads of Department should be able to demonstrate where and how the awareness of risk is imparted to students in lessons.

As well as the programme of training, the school will establish further training or lessons as necessary in response to any incidents.

The e-Safety Officer is responsible for recommending a programme of training and awareness for the school year to the Headmaster for consideration and planning. Should any member of staff feel they have had inadequate or insufficient training generally or in any particular area this must be brought to the attention of the Headmaster for further CPD.

By way of this training, all staff will be made aware that:

Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse

Children can abuse their peers online through:

Abusive, harassing, and misogynistic messages

- Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
- Sharing of abusive images and pornography, to those who don't want to receive such content

Physical abuse, sexual violence and initiation/hazing type violence can all contain an

online element. Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse
- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL and deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

CyberBullying

Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Tutors will discuss cyber-bullying with their tutor groups.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

The school also sends information/leaflets on cyber-bullying to parents/carers so they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will report the incident and provide the relevant material to the police as

soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

Examining electronic devices

The headteacher, and any member of staff authorised to do so by the headteacher, can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. All concerns of this nature should be referred tothe Headteacher and DSL.
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's co-operation

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to the Headteacher and DSL to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

They reasonably suspect that its continued existence is likely to cause harm to any person, and/or

The pupil and/or the parent/carer refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image
- Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Our behaviour policy

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

Artificial intelligence (AI)

Generative AI tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Gemini.

Reading School recognises that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.

Reading School will treat any use of AI to bully pupils very seriously, in line with our behaviour and anti-bullying policies.

Social Networking

Reading School is fully supportive of social networking as a tool to engage and collaborate with learners, and to engage with parents and the wider school community. Any subject specific social media services, permitted for use within Reading School, must have been appropriately risk assessed, managed and moderated in accordance with the Social Media Policies for Staff and Students.

In addition, with reference to images that may be uploaded to such sites, the following is to be strictly adhered to:

- Permission slips (either as hard copy filed in the student record folder or as flagged on the student record on SIMS) must be consulted before any image or video of any child is uploaded.
- There is to be no identification of students using first name and surname; first name only is to be used, if at all.
- All images, videos and other visual resources that are not originated by the school are not allowed unless the owner's permission has been granted.

Permission to use copyrighted resources must be sought and received before they are used.

Social Media: Staff guidance

This guidance applies to teachers, associate staff, governors, those who work on school site (including volunteers that come into contact with pupils) sets out to:

- assist those working with pupils to work online safely and responsibly, to monitor their own standards of behaviour and to prevent the abuse of their position of trust with pupils
- offer a code of practice and a programme of training relevant to their online activities that includes social media for educational, personal and recreational use
- advise that in the event of unsafe and/or unacceptable behaviour disciplinary or legal action (including gross misconduct leading to dismissal) will be taken if necessary in order to support safer working practice
- minimise the risk of malicious allegations against staff and others who have contact with pupils and takes into account the variety of legislation appropriate to this policy.

Use of Social Media and Online Activity of Staff in School

Staff should not access social media sites or engage in other online activity in a personal capacity from the school's computers or other devices at any time unless authorised to do so by a member of the senior management team.

They may use their own computers or other devices while they are in the school to access social media sites or engage in other online activity but only outside of their classroom lesson times. Excessive use of social media which could be considered to interfere with productivity will be considered a disciplinary matter. However, the use of Social Media in a professional capacity and in an educational context is acceptable. In fact, the innovative use of new technologies in the classroom, such as social media, is to be encouraged provided certain safeguards are taken.

Prior to setting up the site, the initiating staff member must discuss the proposed site with, and get authorisation from, their Head of Department and SLT. This discussion should include the proposed content and proposed membership along with the named member of staff who will be responsible for monitoring any pupil uploaded or other content. The method and timing of the content monitoring process needs to be agreed. All this information (and other relevant notes from the initial meeting) should be written up, shared, agreed on and filed for future reference (either electronically or hard copy).

When creating an online social media site (Twitter, Facebook, Flickr, Tumblr, etc.) in an educational context staff must be aware of the setup settings before they allow the site or account to go "live", in particular the privacy settings. If you have any doubts or are uncertain seek the help of the ICT Support Team first.

Any staff using self-created social media sites in a professional capacity must:

- be responsible for the monitoring all content, throughout the site
- be responsible for removing any inappropriate content
- be responsible for restricting the membership of the site members
- ensure that the site is private and cannot be accessed by anyone else, other than the intended members, without invitation

Any staff using any social media sites made in a professional capacity must not:

- Bring the school into disrepute
- Breach confidentiality
- Breach copyrights of any kind
- Bully, harass or be discriminatory in any way
- Be defamatory or derogatory

Use of Social Media& Online Activity Outside of School

The school appreciates that people will make use of social media in a personal capacity. They must be aware that if they are recognised from their profile as being associated with the school then certain opinions expressed could be considered to damage the reputation of the school. A statement such as “the opinions expressed here do not necessarily reflect those of my employer” should be clearly stated and it is advisable to omit any references mentioning the school by name or the person by job title. Opinions should, in any case follow the guidelines above to not bring the school into disrepute, breach confidentiality, breach copyrights or bully, harass or discriminate in any way.

General Considerations for staff (both in and out of School)

When using social media teaching and associate staff should:

- never share work log-in details or passwords
- keep personal phone numbers private
- not give personal email addresses to pupils or parents
- restrict access to certain groups of people on their social media sites and pages.

Those working with children have a duty of care and therefore are expected to adopt high standards of behaviour to retain the confidence and respect of colleagues and pupils both within the school and outside of it. They should maintain appropriate boundaries and manage personal information effectively so that it cannot be misused by third parties for “cyber bullying” for example or possibly identity theft. Staff should not make “friends” of pupils at the school as this could potentially be construed as “grooming”, nor should they accept invitations to become a “friend” of any pupils. Prior to joining the school new employees should check any information they have placed on social media sites and remove any statements that might cause embarrassment or offence.

Staff should use personal mobile phones to contact pupils only as a last resort or in cases where safe guarding is an issue, such as on trips, visits, etc. Staff should keep any communications transparent and on a professional basis by only using the school email addresses, not their personal account. Where there is any doubt

about whether communication between a pupil/parent and member of staff is acceptable and appropriate a member of SLT should be made aware and will decide how to deal with the situation.

Disciplinary Action

Any breaches of this policy relating to social media may lead to disciplinary action under the school's disciplinary Policy. Serious breaches of this policy, for example incidents of bullying of colleagues or social media activity causing serious damage to the organisation, may constitute gross misconduct and lead to dismissal.

Social Media: Student Guidance

When discussing the use of social media by students at Reading School, the following should be noted:

- The use of Facebook, in school hours and in lessons, is blocked on all school owned equipment by our internet filter settings.
- The use of non-RS Twitter accounts, in school hours and in lessons, is not approved and is a behavioural issue rather than an IT issue.
- The use of wireless enabled hand-held devices in school is not banned. We provide a guest wireless network for the sixth form and boarding community.
- The use of 3G + 4G enabled hand held devices in school is banned and their inappropriate use is a behavioural issue that should be logged.

Boarding has a separate policy for the Boarders in relation to internet access. The filtering systemchanges at the end of the school day to allow boarders access to social media sites at the request of the Headmaster and Housemasters.

Personal Capacity

Students should not access social media websites in a personal capacity from the school computers, laptops, tablets or other devices at any time.

They may use their own computers or other devices while they are in the school to access social media websites but only outside of their classroom lesson times. The accessing of social media in the classroom in a personal capacity, rather than as a structured part of a planned lesson, could be considered to interfere with the teaching and learning of the class will be considered a disciplinary matter.

Educational Context

However, the use of Social Media by students, of any age, in an educational context is acceptable. In fact, the innovative use of new technologies by students in the classroom, such as social media, is to be encouraged provided certain safeguards are taken.

When creating, configuring and using an online social media site with students in an educational context, the organising or "moderating" staff will have made those students aware of the setup settings, in particular the privacy settings. Any attempt

by students, either as individuals or as a group, either in school or at home, to circumnavigate or amend or adjust these configurations will be considered a disciplinary matter.

Any pupil using any social media site must:

- act responsibly at all times when on the site
- be responsible for any content they add or upload
- inform at once the “moderator” of any inappropriate content found
- inform at once the “moderator” if they are contacted by someone they do not know
- inform at once the “moderator” if they are suspicious about something

Any pupil using any social media site must not:

- Bring the school into disrepute
- Breach confidentiality
- Breach copyrights of any kind
- Upload inappropriate material or content that refers to the school or any school staff
- Bully, harass or be discriminatory in any way
- Be defamatory or derogatory

Use of Social Media by Students Out of School

Reading School appreciates that students will make use of social media in a personal capacity. However, they must be aware that if they are recognised from their profile as being associated with the school then certain opinions expressed, content added or linked to, or images or movie clips uploaded could be considered as damaging the reputation of the school and may be considered a disciplinary matter.

Content added or uploaded in a personal capacity should follow the Reading School policy guidelines and not bring the school into disrepute, breach confidentiality, breach copyrights or bully, harass or discriminate in any way.

General Considerations (both in and out of School)

When using social media websites, in either a school-based activity or in a personal capacity, students:

- Must never share log-in details or passwords, even with friends or siblings
- Should keep personal phone numbers private
- Should not give out their personal email addresses to any one they do not know
- Should restrict access on their personal social media sites and pages to groups of people they know and trust.
- Must maintain appropriate boundaries and manage personal information effectively so that it cannot be misused by third parties for “cyber bullying” or possibly identity theft.

- Should not invite their teachers or other school staff to be “friends” nor should they accept invitations to become a “friend” of any one they do not know – people online may not be who they say they are, be the age they say they are or even the gender they say they are.
- Should be made aware, when using social media websites, what impression their online presence may give to others. Sixth Formers in particular should take care. All activity on the web leaves an identifiable online footprint, an evidence trail, left behind either as a deliberate act or by association.
- Should, at all times, be made aware and given advice that their online activities can be easily tracked and that this may have a considerable impact on them, either now or in their future aspirations or career choices.

Social media as a forum for parents’ views

It is entirely natural for parents and carers to discuss school life and express their thoughts and opinions with others face to face or on the phone. The school recognises that there will be occasions where, for whatever reason, parents or carers may not agree with a particular course of action or may have specific concerns.

Some of these conversations are now also being aired on social media and the person posting has little control over who might ultimately see it. Some of the comments and observations expressed could cause offence if aired in the public domain, and may in some cases be intimidating or even slanderous.

This is not to suggest that school staff are above criticism or do not welcome feedback. However, it is always best when this is constructive and reasonable and is focused on finding an acceptable solution. When difficult things need to be said, it is usually best to do so face-to-face, or at least in some form of private communication, such as an e-mail or letter.

Ill-considered use of social media can cause school staff to spend a disproportionate amount of time trying to manage issues and situations. The school would much prefer it if this time could be focused on students’ education.

Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 5.

This policy will be reviewed every year by the DSL and safety officer. At every review, the policy will be shared with the governing board. The review (such as the one available here) will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

Appendices

Appendix 2: Staff Agreement for the Use of the ICT at Reading School

Found at [Reading School - Vacancies]

Appendix 3: Pupil Agreement for Use of ICT at Reading School

Agreement Conditions

1. Reading School provides ICT facilities to all students and staff who have been registered with the curriculum network manager by signing and returning their ICT Agreement. As a registered user you may use any these facilities in order to carry out your work, to store files in your own user area on the network, to send and receive emails and to access appropriate information on the Internet.
2. You cannot use any ICT facilities until you are registered and have signed the conditions for use agreement. These conditions are necessary for one or more of the following reasons:
    a. To ensure that all equipment, peripherals, curriculum or administration networks and internet access function properly and are thus available for the benefit of registered users at all times
    b. To ensure that information stored by staff and students is kept safe and available at all times
    c. To comply with the appropriate laws governing the use or misuse of ICT and internet facilities, including the Data Protection Act and school's Data Protection Policy
    d. To ensure that the school and its staff can carry on with their day to day business effectively
3. You should be aware that by signing this agreement you give consent to the network managers and other ICT staff, in the normal pursuit of their work, having access to your user area, your files, to your e-mails. You should also be aware that the time and dates of your network usage are logged and all websites you have visited on the Internet are logged and can be examined. If you break the conditions of the agreement you may be liable to sanctions, up to and including exclusion from the school.

When using Reading School ICT facilities, you MAY:

4. Use the facilities for your schoolwork or for other appropriate work.
5. Send personal e-mails outside of lessons using only the Webmail email system provided with your login account. The sending of emails during lessons, other than class work related messages, is not allowed.
6. Access the Internet providing this does not prevent anyone else from carrying out their work and that such activity falls within the conditions for the use of the facilities.
7. Store only such files as are needed for your work

When using Reading School ICT facilities, you MAY NOT:

8. Send electronic communications which could bring yourself or the school into disrepute or which could render yourself or the school liable to prosecution
9. Knowingly access, view or download any material capable of giving offence
10. Keep, or pass on, e-mails received which contain material capable of giving offence
11. Knowingly import programmes, download files or open attachments that cause viruses to be spread
12. Add to the programs already available to you, either on the network or a stand-alone machine. This includes accessing or downloading games and other programs either from the internet or from other external storage devices (including flash drives, hand held devices, mobile phones or similar)
13. Leave yourself logged in. When away from your station, you must logout.

14. Give your password to any other person or allow them to use your account.
15. Attempt to gain the password of or access the work area of another user.
16. Take part in any other computer related activity which could give offence or bring yourself or the school into disrepute or render yourself or the school liable for prosecution.
17. Attempt to change the operation of any ICT facility by amending its configuration settings, except with the express permission of the network managers or the head of ICT or under instruction of those acting on their behalf
18. Connect any equipment or devices (including flash drives, hand held devices, mobile phones or similar) to any ICT facility, except with the express permission of the network managers or the head of ICT or under instruction of those acting on their behalf.
19. Attempt to circumvent any security systems in place or to be knowingly party to such attempts, either beforeorafter the event.

Appendix 4: Pupil Agreement for Use of ICT at Reading School

Return Slip

Please return in a sealed envelope to the Network Manager

I understand the reasons for regulations governing the use of the ICT facilities at Reading School and I agree to abide by the conditions listed in the agreement. I understand that if I break the rules, access to all ICT facilities, both networked and stand-alone, will be immediately withheld pending investigation. I also understand that any disciplinary action taken against me may, in extreme circumstances, result in my exclusion or dismissal from the school.

Full Name:

(printed please)

Year &Tutor Group:

Student signature: **Date:**

Parent signature: **Date**

User Name (Staff will fill in)

Password (minimum 8 letters/numbers, no spaces, all lower case)

Appendix 5: Guidance for school governors on online social networking produced by the National Co-ordinators of Governor Services (NCOGS)

National Co-ordinators of Governor Serviceshttp://www.ncogs.org.uk/(NCOGS) has produced guidance for school governors on online social networking. It says that social networking sites present an “incredible opportunity” for school governors to communicate and collaborate more effectively, but it notes that these new forms of communication also constitute a risk, and governors should be aware of these implications of participating online in an official capacity.

Disclose your position as a representative of your school It offers the following guidelines on online conduct for school governors: Disclose your status You should disclose your position as a representative of your school unless there are exceptional circumstances, such as a potential threat to personal security. Governors must always be aware that what they say and write as an individual could reflect negatively on them as a governor, their fellow governors or their school. Never give out personal details such as home addresses and phone numbers. Consider the legal framework You should always remember that online participation results in your comments being permanently available and open to being republished in other media. Make sure that you stay within the legal framework and be aware that libel, defamation, copyright and data protection laws apply. This means that you should not disclose information, make commitments or engage in activities on behalf of the school, unless you are authorised to do so. This authority may already be delegated or may be explicitly granted depending on your organisation.

Be aware that libel, defamation, copyright and data protection laws apply Be aware of the media You should also be aware that online participation may attract media interest in you as an individual, so proceed with care whether you are participating in an official or a personal capacity. If you have any doubts, take advice from a colleague.

Acceptable use agreement (staff, governors, volunteers and visitors)

ACCEPTABLE USE OF THE SCHOOL’S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS, VOLUNTEERS AND VISITORS

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS, VOLUNTEERS AND VISITORS	
Name of staff member/governor/volunteer/visitor:	
When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not: • Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material) • Use them in any way which could harm the school's reputation • Access social networking sites or chat rooms • Use any improper language when communicating online, including in emails or other messaging services • Install any unauthorised software, or connect unauthorised hardware or devices to the school's network • Share my password with others or log in to the school's network using someone else's details • Take photographs of pupils without checking with teachers first • Share confidential information about the school, its pupils or staff, or other members of the community • Access, modify or share data I'm not authorised to access, modify or share • Promote private businesses, unless that business is directly related to the school	
I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role. I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy. I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material. I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.	
Signed (staff member/governor/volunteer/visitor):	**Date:**