Founded 1125

Policy number E35

Reading School

E-Safety Policy

Responsibilities	
Policy Owner:	Gareth Sellwood Network Manager
Governors Committee	EXPC

Audit Control	
Policy created:	04/10/2021
Date of next review	Sept/Oct 2023
Version:	1.0
Statutory policy	Yes/No

E-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

Responsibilities

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

Policies Linked

Policy name	File location

Forms Linked

Form name	Form location

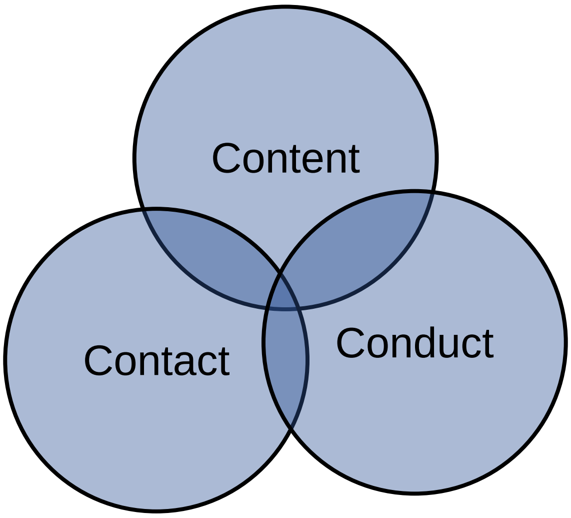
Staff that need to sign

Staff Group	Form location

Contents

Policy 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.



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 twofold:

- To ensure the requirement to empower the whole school community with the knowledge to stay safe and risk free is met.
- 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 more specific 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.

Policy Governance (Roles & Responsibilities)

Governing Body

The governing body is accountable for ensuring that Reading School has effective policies and procedures in place; as such they will:

- Review this policy at least annually and in response to any e-safety incident to ensure that the policy is up to date, covers all aspects of technology use within the school, to ensure e-safety incidents were appropriately dealt with and ensure the policy was effective in managing those incidents.

Individual governors will abide by the guidance for school governors on online social networking produced by the National Co-ordinators of Governor Services (NCOGS), set out in Appendix 6.

Headmaster

Reporting to the governing body, the Headmaster has overall responsibility for e-safety within our school. The day-to-day management of this will be delegated to a member of staff, the e-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.

E-Safety Officer

The designated e-Safety Officer is devolved to Network Manager

The e-Safety Officer will:

- 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
- 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

Staff are to ensure that:

- All details within this policy are understood. If anything is not understood it should be brought to the attention of the Headmaster.
- Any e-safety incident is reported to the e-Safety or in their absence to the Headmaster. If you are unsure the matter is to be raised with the e-Safety Officer or the Headmaster to make a decision.
- The reporting procedure is fully understood

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 son can be granted any access to school network, ICT equipment or services.

The statement set out in Appendix 7 will also be drawn to the attention of parents and carers at appropriate intervals.

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 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.

Safe Use

School Network & the Internet

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.

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.

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.

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.

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 (see Appendix 1). All staff should make themselves aware of the procedures and the responsible staff involved in this process.

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.

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.

Appendix

E-Safety report

1. School E-Safety Incident
2. Staff member reports to Head of House
3. HOH consults E-Safety Officer and sends report
4. Evidence Gathering
5. E-Safety Officer consults SMT member on result

Staff Agreement for the Use of the ICT at Reading School

Staff 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 Manager 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 dismissal.

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 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 e-mails 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 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 Manager or the head of ICT or under instruction of those acting on their behalf
18. Attempt to circumvent any security systems in place or to be knowingly party to such attempts, either before or after the event.

Staff Agreement for the Use of the ICT at Reading School

To be returned to 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.

Staff Agreement

Name………………………………………………………… Initials …………………….

Department ……………………………………………………………….

*User name …………………………………… @reading-school.co.uk

*Password …………………………………………………….

(*leave blank – to be completed by Network Manager)

To be returned to Network Manager

Social Media

Introduction

For the purposes of this policy, social media is defined as interactive online media that allow parties to communicate instantly with one another or share information in a public forum. Examples include Twitter, Facebook and LinkedIn. Social media may also include blogs and video and image-sharing websites such as WordPress, YouTube and Flickr.

Staff should be aware that there are many more examples of social media and this is a constantly developing area of communication. Employees should adhere to these policy guidelines in relation to any social media that they use, in relation to the undertaking of their professional duties and in relation to how the implications of their personal online activity may impact on their professional life.

It is a major contribution to the implementing of e-safety throughout the school, and is an aspect that will be a significant priority for any future OFSTED inspection team.

Scope

Except where more specific applications are given, this policy applies to teachers, associate staff, governors and all who work on the school site, including volunteers, where their work brings them into contact with the pupils.

It 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 & 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. 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

E-safety & Students Working Online

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.

Ofstedcategorises e-safety into 3 areas of risk:

- Content – being exposed to illegal, inappropriate or harmful material.
- Contact – being subjected to harmful online interaction with other users.
- Conduct – personal online behaviour that increases the likelihood of harm.

To keep themselves safe online, both in school and at home, students should be encouraged to:

- use those websites recommended by the teacher initially and be wary of unfamiliar links
- consider who created a website and possible bias within information
- email only people they know and to exercise caution before opening an email sent by someone they don't know
- use Internet chat rooms, websites, instant messaging, etc., with caution and know how to block and report unwanted users
- not use their real name when using games or websites on the Internet, (create a nick name)
- never give out any personal information about themselves, friends or family online including home address, phone or mobile number
- never email your school name or a picture in school uniform (even to a friend)
- never arrange to meet anyone alone, and always tell an adult first and meet in a public place
- only use a webcam with people they know
- tell an adult they trust immediately if they encounter anything they are unhappy with
- report concerns to the Child Exploitation & Online Protection Centre (CEOP)
- avoid using websites they feel they could not tell you about
- be aware comments they make on Blogs and Wikis can be viewed by others

Use of Social Media & Online Activity Outside of School

The school appreciates that people will make use of social media in a personal capacity but 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, so 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 the senior management team should be made aware and will decide how to deal with the situation.

Disciplinary Action

Any breaches of this policy 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.

Staff Social Media Policy – Return Slip

To be returned to the Network Manager

- I have read and understand the School Social Media Policy to which this return slip is attached.
- I have read and understood the e-safety summary section in relation to students safely working online in my classes, when and where appropriate.
- I agree to abide by the conditions listed in the Policy.
- I understand that if I breach the conditions access to all ICT facilities will be immediately withheld pending investigation.
- I understand that any disciplinary action taken against me may, in extreme circumstances, result in my suspension or dismissal from the school.

Name: (print please)

Department:

Date:

Signature:

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.

14. Attempt to gain the password of or access the work area of another user
15. 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
16. 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
17. 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.
18. Attempt to circumvent any security systems in place or to be knowingly party to such attempts, either before orafter the event.

Pupil Agreement for Use of ICT at Reading SchoolReturn 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)

E-Safety Policy

The Use of Social Media by Students

Introduction

For the purposes of this document, social media is defined as interactive online media that allow parties to communicate instantly with one another or share information in a public forum. Examples may include websites such as Twitter, Facebook and LinkedIn. Social media may also include blogs, video and image-sharing websites such as YouTube, Snapchat, Instagram, Tumblr and Flickr.

Staff, both teaching and associate, who are responsible for monitoring the appropriate use of social media websites by students, within school and during school hours, should be aware that there are many, many more examples of social media. This is a constantly developing and rapidly changing area of communication. Students in our care, of all ages, should be made aware of and follow these guidelines in relation to any social media that they use, both in school and at home.

Scope

This policy applies to all students at Reading School, of all ages, and both day boys and Boarders. It is incumbent on all teachers, associate staff, governors and all who work on the school site, including volunteers, to ensure the students in their care are aware of, and adhere to, the guidelines contained within this document.

The policy sets out to:

- To make students more aware of the potential risks online
- To encourage them to monitor their own standards of behaviour whilst online, both in and out of school
- To offer a code of practice, relevant to their use of social media in an educational context, so that they may conduct their online activities in an appropriate and safe way
- To offer advice and provide structured support and make them feel safe whilst online
- To provide students with an awareness of potential risks so that unsafe activity and/or unacceptable behaviour is avoided, either in school or at home

and takes account of the variety of legislation appropriate to this area.

Policy

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 not 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.

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

National Co-ordinators of Governor Services (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.

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.