St. Rose's
Inspiring Education, Therapy & Care

ONLINE SAFETY POLICY

Person responsible:	Vice Principal
Date approved by governing body:	March 2023
Review cycle:	Every year
Date of policy review:	March 2024

St. Rose's
Inspiring Education, Therapy & Care

Online Safety Policy

The policy should be read in conjunction with the following policies:
ICT Policy,
Safeguarding children
Safeguarding adults with care and support needs
Data Breach
Data protection
Information and Records Retention
Information Security
Counter Bullying including cyber bullying
Password
Staff ICT and Internet Acceptable Use
Bring Your Own Device
Also with the following documents:
Keeping Children Safe in Education,
Prevent Risk Assessment
St Rose's and St Martin's E Safety Curriculum
St Rose's and St Martin's PSHE Curriculum
Online safety resources www.saferinternet.org.uk
Student guide to safeguarding St Rose's
Student guide to safeguarding St Martin's

Rationale

New technologies have become integral to the lives of young people in today's society, both within schools and colleges and in their lives outside school and college.

The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and students learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

The aim of the school and college online safety policy is to ensure safe and appropriate ICT use and guard against the dangers that new technologies may bring. The Prevent Duty expects the use of content filtering as a means of restricting access to harmful material online and is paramount in our strategy to prevent people from being drawn into terrorism.

These include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing / distribution of personal images without an individual's consent or knowledge

- Inappropriate communication / contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.
- The danger of becoming radicalized and/or becoming involved in extremism by online videos or through social media

As with all other risks, it is impossible to eliminate those risks completely. We will therefore aim through good educational provision to build the resilience of students to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

The school and college will provide the necessary safeguards to help ensure that we manage and reduce these risks.

Scope of the Policy

This policy applies to all members of St Rose's community (including staff, young people, volunteers, parents / carers, visitors, community users) who have access to and are users of St Rose's ICT systems, both in and out of school and college.

The Education and Inspections Act 2006 empowers Principals, to such extent as is reasonable, to regulate the behaviour of young people when they are off the school and college site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other online safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school and college.

St Rose's will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate online safety behaviour that take place out of school and college.

Roles and Responsibilities

The Principal is responsible for ensuring the safety (including online safety) of members of the school and college community, though the day to day responsibility for online safety will be delegated to the Online Safety Lead.

In the event of an online safety incident taking place the member of staff would report the online safety incident to the Principal/ Online safety Coordinator and a log of the incident would be created and appropriate action taken by the Principal. The SCMT will regularly review online safety incidents to inform future online safety developments.

The IT Manager is responsible for ensuring that the ICT infrastructure is secure and is not open to misuse or malicious attack and that the school meets the online safety technical requirements as required by this policy.

All staff are responsible for ensuring that:

- They have an up to date awareness of online safety matters and of the current St Rose's online safety policy and practices
- They have read, understood and signed the Staff ICT and Internet Acceptable Use Policy and current IT Password Policy
- They must monitor ICT activity in lessons, extracurricular and extended school activities
- They must report any suspected misuse or problem to the Principal for investigation

The students who can understand the issues are responsible for using the ICT systems in accordance with the ICT Usage Agreement (see Appendix), which they will be expected to sign before being given access to the systems. It would be expected that parents / carers would sign on behalf of many of our students.

Parents and carers will be responsible for endorsing (by signature) the ICT Usage Agreement

Education

Pupils and students will receive Online safety education in the following ways:-

- A planned online safety programme is provided and delivered as part of ICT and PHSE and should be regularly revisited – this will cover both the use of ICT and new technologies in and outside St Rose's.
- Opportunities in our Pathway 1 formal curriculum lessons including English, mathematics, RE, humanities and science lessons, where students are accessing ICT, will also be used to discuss online safety where appropriate.
- Young people will be taught at all times to be critically aware of the materials / content they access online and be guided to validate the accuracy of information

The school and college will provide information and awareness to parents and carers.

All new staff will receive online safety training as part of their induction programme, ensuring that they fully understand the Online Safety Policy, Staff ICT and Internet Acceptable Use Policy and current IT Password Policy.

ICT Infrastructure, content filtering and monitoring

The school and college will be responsible for ensuring that the network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities.

ICT systems will be managed in ways that ensure that St Rose's meets the online safety technical requirements outlined in the Information Security Policy and Staff ICT and Internet Acceptable Use Policy and any relevant Local Authority online safety policy and guidance.

There will be regular reviews and audits of the safety and security of ICT systems.

The nature of our school and college and students' difficulty for the majority of them to access computers completely independently means that we have a general user log in for our students with a password which gives access to the student files, photos and internet. Some students, *where appropriate are given their own log in to access the system. There is an understanding that students will not access the internet in an unsupervised situation unless they have been given permission.*

Users will be responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security. St Rose's has provided enhanced content filtering through the use of EXA Networks SurfProtect filtering system.

In the event of the IT Manager needing to manage the filtering for any reason, or for any user, this will be logged and carried out according to a process that is agreed by the Principal.

Requests from staff for sites to be removed from the filtered list will be considered by the IT Manager who will seek advice from the Online Safety Lead. If the request is agreed, this action will be recorded and logs of such actions will be reviewed termly by the Online Safety Lead.

The IT Manager will regularly monitor and record the activity of staff on the ICT systems and users are made aware of this in the Staff ICT and Internet Acceptable Use Policy agreements.

Remote management tools can be used by IT staff to control workstations and view users Activity at any time.

Staff are able to report any actual / potential online safety incident to the IT Manager or Online Safety Lead who logs their concern and contacts the Principal.

The IT Manager will ensure that appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, workstations, mobile devices etc. from accidental or malicious attempts to threaten the security of the systems and data.

The IT Manager will ensure that the school infrastructure and individual workstations are protected by an up-to-date anti-virus software.

Staff must contact the IT Manager for advice before downloading executable files (.exe)

Laptops and other mobile devices that are the property of St Rose's are only for the use of the member of staff which it is assigned to when they are out of the school/college.

Staff are not allowed to install software on school/college workstations/mobile devices.

Staff must use password protected encrypted memory sticks supplied by the IT team on workstations/portable devices should they be required.

They may use pre-recorded CDs and DVDs without restriction.

Personal data e.g. name, address, DOB etc. must not be sent over the internet (e.g. sent as an e-mail attachment) or taken off the school site unless safely encrypted.

Mobile Device Management

The school utilises Apple iPads as learning and communication aids and there are particular safeguards in place for these devices.

iPads users should not:

- *Add or remove applications*
- *Create an Apple ID/iTunes account*
- *Change any configuration settings on the iPad*
- *Jailbreak the iPad*
- *Erase the iPad on another computer*
- *Synchronise the iPad with a computer outside of school*
- *Change or disable the access password, or PIN on the iPad*
- *Store or leave an iPad unattended in a vehicle*

Curriculum

Online safety is a focus in all areas of the curriculum and staff will reinforce online safety messages in the use of ICT across the curriculum. The prevention of radicalisation and extremism through online videos or social media are addressed through the PSHE curriculum.

Use of digital photos and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and young people instant use of images that they have recorded themselves or downloaded from the internet. However, staff and young people need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. When using digital images, staff will, where appropriate, inform and educate young people about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.

Staff are allowed to take digital / video images to support educational aims, but must follow the St Rose's policies concerning the sharing, distribution and publication of those images. Those images should only be taken on the school's equipment, the personal equipment of staff should not be used for such purposes unless permission has been given in accordance with the Staff ICT and Internet Acceptable Use Policy agreement.

Students must not use, share, publish or distribute images of others without their permission. Photographs published on the website, or elsewhere that include young people will be selected carefully and will comply with good practice guidance on the use of such images. Photographs on the website will only be used with parental permission. Young people's full names will not be used anywhere on a website or blog, particularly in association with photographs. Young people's work can only be published with the permission of the student and parents or carers.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the principles of the General Data Protection Regulation 2018 which states that personal data must be:

- Processed lawfully, fairly and in a transparent way in relation to individuals
- Collected for specific, explicit, and authentic purposes
- Adequate, relevant, and limited to what is needed
- Accurate and kept up-to-date

- Retained only for as long as necessary
- Processed in a way to maintain security

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks / disadvantages

	Staff & other adults				Students / Pupils			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission/supervision	Not allowed
Mobile phones may be brought to school	√				√			
Use of mobile phones in lessons				√				√
Use of personal mobile phones during working time			√ *				√	
Use of VOCA to take photos	√						√	
Taking photos on mobile phones or other camera devices		√*						√
Use of personal email addresses in school, or on school network				√			√	
Use of school email for personal emails				√	√			
Use of chat rooms / facilities				√				√
Use of instant messaging				√			√	
Use of social networking sites				√			√	
Use of blogs			√				√	
Use of young person's mobile phone			√			√		

**Assume not allowed unless you have been given permission by the Leadership and Management Team.*

When using communication technologies, the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored.
- Users need to be aware that email communications may be monitored
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff and students / pupils or parents / carers (email, chat, VLE etc) must be professional in tone and content.

Unsuitable or inappropriate activity

Activities referred to in the following section would be inappropriate and that users, as defined below, should not engage in these activities when using the school's equipment or systems.

User Actions

		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	child sexual abuse images					√
	promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse and fraud legislation					√
	adult material that potentially breaches the Obscene Publications Act in the UK					√
	criminally racist material in UK					√
	Promotion of extremism or terrorism				√	
	Pornography				√	
	promotion of any kind of discrimination				√	
	promotion of racial or religious hatred				√	
	threatening behaviour, including promotion of physical violence or mental harm				√	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				√	
Using school systems to run a private business					√	
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school					√	
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions					√	
Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)					√	
Creating or propagating computer viruses or other harmful files					√	
Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet					√	

On-line gaming (educational) Acceptable with supervision	√			
On-line gaming (non educational) Acceptable with supervision	√			
On-line gambling				√
On-line shopping / commerce	√ staff			√ pupils
File sharing	√			
Use of social networking sites				√
Use of video broadcasting e.g. YouTube Acceptable with supervision	√			

Responding to incidents of misuse

Listed below are the responses that will be made to any apparent or actual incidents of misuse:

Illegal activity:- If any apparent or actual misuse appears to involve illegal activity i.e.

- child sexual abuse images
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials

The Principal should be informed immediately and take appropriate action.

Inappropriate Activity:-

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school are aware that incidents have been dealt with. Other incidents of misuse will be dealt with as follows:

Young people Actions / Sanctions

Incidents:	Refer to class teacher / tutor	Refer to Head of Department / Head of Year / other	Refer to Principal	Refer to Police	Refer to technical support staff for action re filtering / security etc	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction e.g. detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		√	√	√					
Unauthorised use of non-educational sites during lessons	√		√						
Unauthorised use of mobile phone / digital camera / other handheld device	√		√						
Unauthorised use of social networking / instant messaging / personal email	√		√						
Unauthorised downloading or uploading of files	√		√		√				
Allowing others to access school network by sharing username and passwords	√		√		√				
Attempting to access or accessing the school/college network, using another student's account	√		√						

Attempting to access or accessing the school network, using the account of a member of staff	√		√		√				
Corrupting or destroying the data of other users	√		√		√				
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	√		√			√			
Continued infringements of the above, following previous warnings or sanctions	√		√			√	√		
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	√		√		√	√			
Using proxy sites or other means to subvert the school's filtering system	√		√		√				
Accidentally accessing offensive or pornographic material and failing to report the incident	√		√		√				
Deliberately accessing or trying to access offensive or pornographic material	√		√	√	√	√	√		
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	√		√	√	√		√		

Staff

Incidents:	Refer to line manager	Refer to Principal	Refer to Police	Refer to Technical Support Staff for action re filtering etc
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		√	√	
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email		√		√
Unauthorised downloading or uploading of files		√		√
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account		√		√
Careless use of personal data e.g. holding or transferring data in an insecure manner		√		√
Deliberate actions to breach data protection or network security rules		√		√
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		√		√
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature		√		
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils		√		√
Actions which could compromise the staff member's professional standing		√		

Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		√		
Using proxy sites or other means to subvert the school's filtering system		√		√
Accidentally accessing offensive or pornographic material and failing to report the incident		√		√
Deliberately accessing or trying to access offensive or pornographic material		√	√	√
Breaching copyright or licensing regulations		√		√
Continued infringements of the above, following previous warnings or sanctions		√		

NB If the allegation is involving the Principal then the designated safeguarding officer would contact the Local Authority Designated Officer (LADO) and the Chair of Governors.

Acknowledgements

This policy has been based on the Self Review Framework produced by SWGfL.

Appendix

Staff ICT and Internet Acceptable Use Policy Agreement
IT Password Policy
Young people and/or Parents/Carers ICT Usage Agreement

APPENDIX

St. Rose's
Inspiring Education, Therapy & Care

March 2021

St Rose's and St Martin's

ICT USAGE AGREEMENT

Rules for Safe and Responsible Computer and Internet Use

- I will not access other people's files
- I will only use the computers for school/college work or approved activities
- I will not bring in any USB stick or other media from outside school/college without permission
- I will not use the Internet without a member of staff in the room, unless I have been given permission
- I will only email people I know, or my teacher has approved
- The messages I send will be polite and responsible
- I will not give my home address, telephone number or arrange to meet anyone over the internet
- I will report any unpleasant material or messages sent to me. I understand my report would be confidential and would protect other students and myself
- I understand that St Rose's or St Martin's may check my computer files and may monitor my use of the Internet
- I understand that if I deliberately break these rules I could be stopped from using computers at St Rose's or St Martin's
- I understand that I can only use social networking sites with staff permission/supervision

AGREEMENT

Student (where applicable)

As a user of the St Rose's or St Martin's network I agree to abide by the rules above, which are there to keep everyone safe and to help us to be fair to others.

Name: ………………………………………

Signed: ……………………………………… **Class: ……………………….** **Date: …………………….**

Parent

As a parent of a student at St Rose's or St Martin's, I grant permission for my son/daughter to use email and the Internet, in a supervised situation. I have read and understood the above.

Name: ……………………………………… **Signed: ……………………………….**

Date: ………………………………………

Everything that happens in St Rose's should remain confidential. Staff must not talk about St Rose's with colleagues on social internet sites e.g. Facebook.

This Policy Statement is considered part of the Terms and Conditions of Employment for all staff at St Rose's.

………………………………………… Chair of Governors Date 15-3. 2023 **……………………………**

J. Talwar **………………………………………… Principal Date** 15.3.2023 **……………………………**