Online Safety Policy and Procedure

Date approved by Trustees	April 2018
Date for next review	April 2020
Compliance lead	Trust Head of IT and MIS
Agreed Policy file name	Online Safety Policy and Procedure
Agreed policy location:	RMT Information area\Policies and Procedures (internal access only

POLICY:

New technologies have become integral to the lives of children and adults in today's society, both within Ruskin Mill provisions and in their lives outside the provision.

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

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in the Ruskin Mill Trust provisions are bound. The online safety policy should help to ensure safe and appropriate use. The development and implementation of such a strategy should involve all the stakeholders in a student's education from the principal and Trustees to the senior leaders and tutors, support staff, parents, members of the community and the students themselves.

Appropriate use of these exciting and innovative tools in the provision and at home has been shown to raise educational standards and promote student achievement. However, the use of these new technologies can put children and adults at risk within and outside the provision. Some of the dangers they may face 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.
- Potential for radicalisation through inappropriate content or contact.

Many of these risks reflect situations in the off-line world and it is essential that this online safety policy is used in conjunction with other Trust policies e.g. safeguarding policy and social media policy.

As with all risks, it is impossible to eliminate them completely. It is therefore essential, through good educational provision to build students' resilience 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 Trust will provide the necessary safeguards to help ensure that it has done everything that could reasonably be expected of it to manage and reduce these risks.

The Trust's online safety policy explains how it intends to manage risk, while also addressing wider educational issues in order to help young people to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

PROCEDURES

Students - education

Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students in online safety is therefore an essential part of the Trust's online safety provision. Children and young people need the help and support of their provision to recognise and avoid online safety risks and build their resilience.

Online Safety education will be provided in the following ways:

- Key online safety messages should be reinforced as part of a planned programme of tutorials and pastoral activities
- Students should be taught in relevant sessions to be critically aware of the materials/ content they access on-line and be guided to validate the accuracy of information
- Students should be helped to understand the need for the student AUP and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside their provision
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Students should be taught the dangers that can exist through the use of inappropriate websites, and the potential of on-line grooming for exploitation or radicalisation purposes
- Staff should act as good role models in their use of ICT, the internet and mobile devices

Staff - education & training

- This Online Safety policy and its updates will be presented to and discussed at relevant team meetings in conjunction with the Social Media Policy and Procedure.
- Technical – infrastructure / equipment, filtering and monitoring
- The Trust will be responsible for ensuring that the Trust network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented:
- There will be regular reviews and audits of the safety and security of Trust ICT systems
- Servers, and wireless systems must be securely located and physical access restricted
- All users will have clearly defined access rights to the Trust's ICT systems.

- All users will be provided with a username and password by the technical services team who will keep an up to date record of users and their usernames.
- The “master / administrator” passwords for the Trust’s ICT systems, used by the Network Manager (or other person) must also be available to the Trust Head of IT and MIS for auditing purposes
- Users will be made 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.
- The Trust has provided enhanced user-level filtering through the use of the eSafe Systems Ltd filtering programme.
- Trust ICT technical staff monitor and record the activity of users on the Trust ICT systems and users are made aware of this in the Acceptable Use Policy, this includes monitoring related to child safety, bullying and radicalisation.
- Remote management tools are used by staff to control workstations and view users activity with their permission
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices and other relevant equipment from accidental or malicious attempts which might threaten the security of the Trust systems and data.
- An agreed policy is in place regarding the downloading software by users (Within the AUP)
- An agreed policy is in place that forbids staff from installing programmes on Trust workstations / portable devices. (Within the AUP)
- The Trust’s infrastructure and individual workstations are protected by up to date virus software.
- Personal data may not be sent over the internet or taken away from a Trust site unless safely encrypted or otherwise secured.

IMPACT OF NON-COMPLIANCE FOR:

Staff	Disciplinary action
Students	Risk of harm
Legislation / organisation	Reputational damage, litigation

Appendix 1 – Safeguarding Yourself as an employee of the Trust

Guidance on the personal use of social networking sites for adults involved in services for children, young people and vulnerable adults

Due to the increasing personal use of social networking sites, staff and volunteers within the workforce should be aware of the impact of their personal use upon their professional position.

In practice, anything posted on the internet will be there forever and is no longer in your control. Remember when something is on the internet even if you remove it, it may have already been "snapshotted" by a "web crawler" and so will always be there.

Current and future employers and service users may see this. Keep all professional work completely separate from your private life.

The following guidance, in addition to the above, will safeguard adults from allegations and protect an individual's privacy as well as safeguard vulnerable groups.

Failure to comply with the following may result in organisations taking disciplinary action.

- Social networking sites such as facebook have a range of privacy settings which are often set up to 'expose' your details to anyone. When 'open' anyone can find you from a search of the social networking site or even from a Google search. Therefore, it is important to change your setting to 'just friends' so that your details, comments, photographs can only be seen your invited friends
- Have a neutral picture of yourself as your profile image
- Do not post embarrassing material or comments that may call into question your employment status, this includes anything that is confidential or sensitive including information about students or ex-students, any information that is intended for internal use only (including matters concerning provision services, organisational change or related proposals)
- You should always show respect to others when using social media. You must never criticise the Trust, its students and staff or anyone else you come into contact with professionally.
- Do not use personal social media to raise or discuss a complaint or grievance about the Trust, your manager, colleagues etc. There are formal grievance procedures for progressing these within the Trust.
- Do not accept friendship requests unless you know the person or want to accept them
- Be prepared for being bombarded with friendship requests from people you do not know
- Do not make friendship requests with students
- Choose your social networking friends carefully and ask about their privacy controls
- Do not accept friendship requests on social networking or messaging sites from students (or their parents) or service users that you work with.
- For those working with young people remember that ex pupils may still have friends that you may have contact with through your work
- Exercise caution. For example, if you write on a friends 'wall' on facebook all of their friends can see your comment even if they are not your friend
- There is a separate privacy setting for facebook groups and networks.
- You may have your own profile set to private, however, when joining a group or a network please be aware that everyone in that group or network is able to see your profile
- If you have younger friends or family members on your social networking groups who are friends with students, pupils, young people (or their parents) or service users that you work with, be aware that posts you write will be visible to them

- Do not use your personal or professional details (email or telephone) as part of your profile
- If you or a friend are tagged in an online photo album (facebook, flickr) the whole photo album may be visible to their friends, your friends and anyone else tagged in the photo album
- You do not have to be friends with anyone to be tagged in their photo album, if you are tagged in a photo you can remove the tag but not the photo
- You should be aware of the privacy settings on photo sharing websites
- Your friends may take and post photos that you may not be happy about. You need to speak to them first to request that it is removed rather than contacting the web provider. If you are over the age of 18, the website will only look into issues that contravene their terms and conditions
- Do not use your personal profile in any way for official business. If you are going to be a friend of your organisations official social networking group ensure you have a separate professional profile
- If you have concerns related to radicalisation or on-line grooming then please contact the local safeguarding lead.
- If you have difficulty in implementing any of this guidance contact the local safeguarding lead.