ROTHERHAM UNITED COMMUNITY TRUST

POLICY / PROCEDURE

NAME: E-Safety
VERSION: V2

Written by	James Mahoney
Creation date	October 2016
Signed by trustee	
Date signed	
Review frequency	Annually
Revision details	

E-Safety Policy

Rotherham United Community Trust

Introduction

Rotherham United Community Trust recognises the benefits and opportunities which new technologies offer to teaching and learning. Our approach is to implement safeguards within the organisation, and to support staff and learners to identify and manage risks. We believe this can be achieved through a combination of security measures, training and guidance and implementation of our associated policies.

We will do all that we can to make our learners and staff stay 'e-safe' and to satisfy our wider duty of care.

This e-safety policy should be read in conjunction with other relevant RUCT policies procedures such as Safeguarding, Anti - Bullying Policy, and RUCT Disciplinary Policies.

Definition of E-Safety

The term e-safety is defined for the purposes of this document as the process of limiting the risks to children, young people and vulnerable Adults when using Internet, Digital and Mobile Technologies (IDMTs) through a combined approach to policies and procedures, infrastructures and education, including training, underpinned by standards and inspection.

E-safety risks can be summarised under the following three headings.

- Exposure to age-inappropriate material
- Exposure to inaccurate or misleading information
- Exposure to socially unacceptable material, such as that inciting violence, hate, extremism or intolerance
- Exposure to illegal material, such as images of child abuse
- Illegal Downloading of copyrighted materials e.g. music and films
- Grooming using communication technologies, potentially leading to sexual assault or child prostitution
- Radicalisation the process by which a person comes to support terrorism and extremist ideologies associated with terrorist groups.
- Bullying via websites, mobile phones or other forms of communication device
- Exposure of minors to inappropriate commercial advertising
- Exposure to online gambling services
- Commercial and financial scams

Scope

The policy applies to all persons who have access to College IT systems, both on premises and remote access. Any user of RUCT IT systems must adhere to e-Safety Rules.

The e-Safety Policy applies to all use of the internet, and electronic communication devices such as email, mobile phones, games consoles, social networking sites, and any other systems that use the internet for connection and providing of information.

Aims

The aims are to:

- To ensure safeguards on RUCT IT-based systems are strong and reliable
- To ensure user behaviour is safe and appropriate
- To assure that the storage and use of images and personal information on College IT based systems is secure and meets all legal requirements
- To educate Staff and learners in e-safety
- To ensure any incidents which threaten e-safety are managed appropriately

Security

RUCT networks are safe and secure, with appropriate and up-to-date security measures and software in place.

Risk assessment

When making use of new technologies and online platforms, staff are to assess the potential risks that they and their learners could be exposed to.

Behaviour

- It is unacceptable to download or transmit any material which might reasonably be considered obscene, abusive, sexist, racist, defamatory, related to violent extremism or terrorism or which is intended to annoy, harass or intimidate another person. This also applies to use of social media systems accessed from College systems.
- All users of IT adhere to College guidelines when using email, mobile phones, social networking sites, games consoles, chat rooms, video conferencing and web cameras, etc.
- Any abuse of IT systems and any issues of bullying or harassment (cyber bullying) are dealt with seriously, in line with staff and student disciplinary procedures.
- Any conduct considered illegal is reported to the police.
- Staff must take responsibility for moderating any content posted online.
- Staff should be aware of cyber bullying, grooming law and child protection issues and forward any concerns to the Lead Safeguarding Manager.
- Staff should keep personal and professional lives separate online.
- Staff should not have students as ‘friends’ on social media sites that share personal information.
- Staff should be wary of divulging personal details online and are advised to look into privacy settings on sites to control what information is publicly accessible.
- Staff should recognise that they are legally liable for anything they post online.
- Staff are expected to adhere to the college’s equality and diversity policy at all times and not post derogatory, offensive or prejudiced comments online.
- Staff should not bully or abuse colleagues/students online.
- Staff entering into a debate with a student online should ensure that their comments reflect a professional approach.
- Staff should not post any comments online that may bring the college into disrepute or that may damage the college’s reputation.
- Staff wishing to debate and comment on professional issues using personal sites, should be aware that this may be seen as a reflection of college views, even with a disclaimer, and should consider their postings carefully.
- Staff should not use their college e-mail address to join sites for personal reasons or make their college e-mail address their primary contact method.
- Staff should be aware that any reports of them undertaking inappropriate online activity that links them to the College will be investigated and may result in disciplinary action.

Use of images and video

- The use of images or photographs is encouraged in teaching and learning, providing there is no breach of copyright or other rights of another person.
- Staff and learners are trained in the risks in downloading, posting and sharing images, and particularly in the risks involved in posting personal images onto social networking sites.
- College staff provide information to learners on the appropriate use of images, and on how to keep their personal information safe.
- Advice and approval from a senior manager is sought in specified circumstances or if there is any doubt about the publication of any materials.

Personal information

- Processing of personal information is done in compliance with the Data Protection Act 2018.
- Personal information is kept safe and secure and is not passed on to anyone else without the express permission of the individual.
- No personal information is posted to the RUCT website/intranets without the permission of a senior manager.
- Staff keep learners' personal information safe and secure at all times.
- When using an online platform, all personal information is password protected.
- No personal information of individuals is taken offsite unless the member of staff has the permission of their manager.
- Every user of IT facilities logs off on completion of any activity, or ensures rooms are locked if unsupervised, where they are physically absent from a device.
- College mobile devices that store sensitive information are encrypted and password protected.
- Personal data no longer required, is securely deleted.

Education and Training

- Staff and learners are supported through training and education to develop the skills to be able to identify risks independently and manage them effectively.
- Learner inductions and the tutorial programme contains sessions on e-safety.
- Learners are guided in e-safety across the curriculum and opportunities are taken to reinforce e-safety messages.
- Learners know what to do and who to talk to where they have concerns about inappropriate content, either where that material is directed to them, or where it is discovered as part of a random search.
- In classes, learners are encouraged to question the validity and reliability of materials researched, viewed or downloaded. They are encouraged to respect the copyright of other parties and to cite references properly.

Incidents and Response

A clear and effective incident reporting procedure is maintained and communicated to learners and staff. Reports of e-safety incidents are acted upon immediately to prevent, as far as reasonably possible, any harm or further harm occurring. Action following the report of an incident might include disciplinary action, sanctions, reports to external agencies (e.g. the police), review of internal procedures and safeguards, tutor support for affected learners, etc.

Responsibilities

The Head of IT Services and Lead Safeguarding Manager are responsible for maintaining this policy, and for maintaining best practice in IT procedures and practices to manage any e-safety risks effectively.

The following are responsible for implementing it:

- The Director of Human Resources for all e-safety matters in relation to RUCT Staff.

- Lead Safeguarding Manager for all e-safety matters in relation to RUCT
- Learners.
- The Head of IT Services for championing good e-safety practice in RUCT IT facilities and processes, and for providing technical expertise when issues are being investigated.
- All tutors for embedding e-safety education and practice into their teaching programme.
- All RUCT Managers for implementing good e-safety practice and safeguards consistent with this policy in their area of responsibility.
- The RUCT Safeguarding Committee for overseeing and reviewing e-safety arrangements.
- All members of college staff for staying alert to and responding appropriately to any potential or actual e-safety issue.

Access to the Policy

The policy will be available to staff within the internal shared drive and to students via Google Classroom.

Monitoring and Review

The impact of the policy will be monitored regularly with a full review being carried out at least once every year. The policy will also be reviewed where concerns are raised by the Safeguarding Manager, or where an e-safety incident has been recorded.