Online Safety

Date created:
June 2023

Date for Review:
June 2024

Version:
1

Policies & Procedures

Online Safety Policy

Introduction

New technologies have become integral to the lives of children and adult sin today's society. The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teaching staff and students learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children, young people 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 communication technologies appropriately and safely is addressed as part of the wider duty of care to which all who at Rotherham Opportunities College are bound. The online safety policy should help to ensure safe and appropriate use. The development and implementation of such a policy should involve all the stakeholders in a student's education from the Directors and senior leaders to the teachers, support staff, parents/carers, members of the community and the students themselves.

Potential Dangers

Appropriate use of these exciting and innovative tools has been shown to raise educational standards and promote student achievement. However, the use of these new technologies can put people at risk within and outside the organisation. Some of the dangers individuals 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 situation in the off-line world and it is essential that this online safety policy is used in conjunction with other relevant college policies e.g. Safeguarding policy and Prevent policy.

As with all risk, it is impossible to eliminate them completely. It is therefore essential, through good education to build students' resilience to the risks to which they may be exposes, so they have the confidence and skills to face and deal with these risks.

The college 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 college'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

Whilst regulation and technical solutions are very important, their use must be balance by education students to take a responsible approach. The education of students in online safety is therefore an essential part of the college's online safety provision. Students need the help and support of the college 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 reinforces as part of a planned programme of tutorial and teaching 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 the 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 educational 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, 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

Staff must familiarise themselves with this policy and on how to safeguard themselves as a staff member of Rotherham Opportunities College.

- This online safety policy and its updates will be presented to and discussed at relevant team meetings in conjunction with the Acceptable Use Policy and the Safeguarding policy.
- Technical infrastructure / equipment will enable filtering and monitoring by Rotherham Opportunities College;
- The college will be responsible for ensuring that the college network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented;
- Regular reviews and audits of the safety and security of the ICT systems;
- Servers and wireless systems must be securely located and physical access restricted;
- All users will have clearly defined access rights to the college's ICT systems;
- All users will be provided with a username and password by the Technical Services Manager who will keep an up to date record of users and their usernames;
- Users will be held responsible for the security of their username and password and must not allow other users to access the systems using their long on details and must immediately report any suspicion or evidence that there has been a break of security;
- The college has provided enhanced user- level filtering through the sue of a filtering programme;
- The Technical Services Manger monitor and record the activity of users on the ICT systems and users are made aware of this in the

Acceptable Use Policy.; this includes monitoring related to bullying, radicalisation and child safety;

- 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 systems and data;
- An agreed policy is in place that forbids staff from installing programmes on workstations / portable devices (within AUP);
- The college's infrastructure e 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.