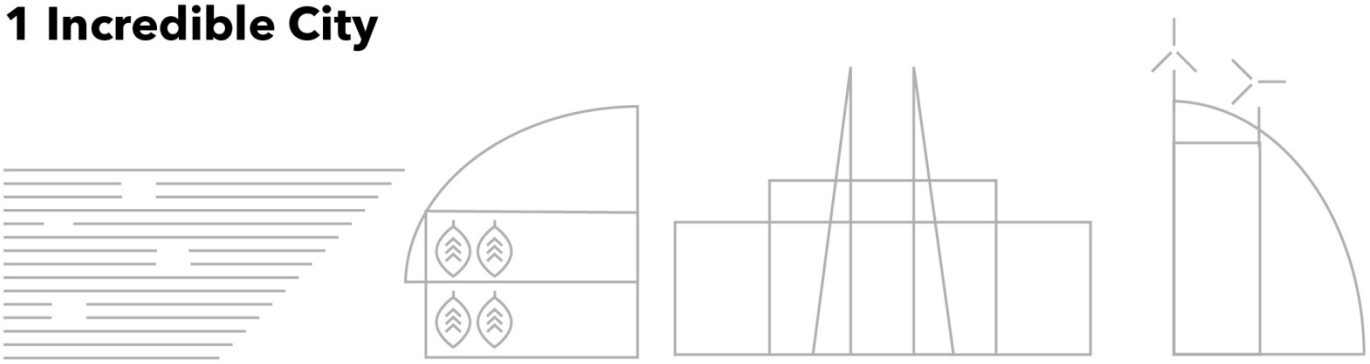
The Sheffield College

Online Safety Policy

4 Excellent Centres
1000's of Opportunities
1 Incredible City



The Sheffield College

Document Information:

Author: Caroline Morrison, Martin Plummer

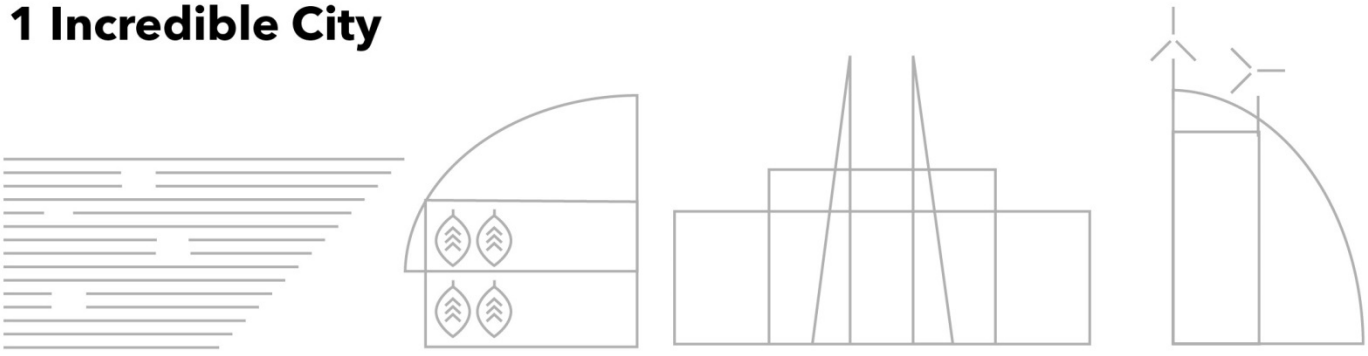
Date Issued: December 2017

Date Approved and endorsed: Awaiting re-approval

Filename: TSC Online Safety Policy 2017-18

File Location: G: Student Services & Support/Policies

4 Excellent Centres
1000's of Opportunities
1 Incredible City



Online Safety Policy

Document Author:	Position:	Date of Issue:	Issue No.:	File Name:
Caroline Morrison, Martin Plummer	Assistant Principal IT Manager	December 2017	002	TSC Online Safety Policy 2017-18
Endorsed By:	The Safeguarding Board			**Date of Approval/Endorsement:** Awaiting re-approval
Approved By:	The Sheffield College Student Union			**Date of Approval/Endorsement:** Awaiting re-approval

The Sheffield College Online Safety Policy

1 An Overview of the Risks

ICT can offer many positive educational and social benefits to young people; however, unfortunately there are some dangers. As in any other area of life, young people and vulnerable adults may expose themselves to danger, whether knowingly or unknowingly, when using the internet and other technologies. Additionally, some young people may find themselves involved in activities, which are inappropriate, or possibly illegal.

The Sheffield College recognises the benefits and opportunities, which new technologies offer to teaching, learning and work productivity. We provide internet access to all learners and staff and encourage the use of technologies in order to enhance skills/work-ethic, promote achievement and enable lifelong learning. A proportion of many of our curriculum courses are delivered online as are opportunities for staff professional development training. However, the accessibility, global nature of the internet and different technologies available mean that we are also aware of potential risks and challenges associated with such use.

Our approach is to implement appropriate safeguards within the College while supporting staff and students to identify and manage risks independently, with confidence. We believe this can be achieved through a combination of security measures, training, guidance and implementation of our policies.

In furtherance of our duty to safeguard students, and to satisfy our wider duty of care, we will do all we can to make our students and staff stay safe online. This Online Safety policy should be read alongside other relevant college policies, including:

- Safeguarding Policy
- Prevent Strategy
- Prevent Risk Assessment
- Student Positive Engagement Policy and Procedure
- ICT Facilities Access Regulations (IFAR)
- Social Media Policy
- Bring Your Own Device (BYOD) Acceptable Use Policy
- Use of Photos, Videos and Media Acceptable Use Policy
- Cloud Computing Acceptable Use Policy

2 Creation, Monitoring and Review

ICT Systems, the Online College Team, librarians**,** teaching and learning staff and representatives from Sheffield College's Student Union have contributed to the online safety policy. The designated Lead Safeguarding, Officer Caroline Morrison, and the IT Manager, Martin Plummer, oversee the Online Safety policy. It has been developed using national Online Safety guidance, the Sheffield Safeguarding Children Board advice and examples of Further Education related best practice.

The Sheffield College Safeguarding Board will monitor the impact of the policy biannually and the policy will be reviewed annually. The foundation of the Online

Safety policy is the college's Online Safety self-assessment (Appendix 1), which analyses our provision and RAG rates it in terms of compliance. Any areas noted as Red or Amber are logged for development to improve the protection and education of both our students and staff, with associated actions and timeframes.

3 Scope of the Policy

This policy applies to all students, staff and members of the College community who have access to the College IT systems and /or the Internet, both on premises and remotely. Any user of College IT systems must adhere to the ICT Facilities Access Regulations (IFAR) and this Online Safety policy.

This policy applies to all use of the internet and forms of electronic communications such as email, cloud computing, mobile technology, Bring Your Own Device (BYOD), social media sites and instant messaging.

4 Roles and Responsibilities

There are clear lines of responsibility for Online Safety within the College. All members of the College community are responsible for ensuring the Online Safety of themselves and others in College and on College related activities. Concerns should be reported immediately to a member of the Safeguarding Team. When informed about an incident staff should take care not to guarantee confidentiality towards the individual that reported it or those involved.

4.1 Online Safety Coordinator

The Online Safety Coordinator is responsible for keeping up to date with new technologies and their use as well as attending relevant training. They will be expected to lead the Online Safety review process, provide updates to the Online Safety Policy when required, deliver staff/parent development/ training, record incidents, and liaise with the local authority and external agencies to promote Online Safety within the College community. The Online Safety Coordinator role for The Sheffield College is a shared between Caroline Morrison (Assistant Principal), Martin Plummer (IT Manager) and Kieran Briggs (Digital and E Learning Coordinator)

4.2 Students

Students are responsible for using the College IT systems and mobile devices in accordance with the College's ICT Facilities Access Regulations (IFAR) user agreement. They must sign to declare at the time of registration.

Learners must act safely and responsibly at all times when using the internet and/or mobile technologies both in learning and social contexts, in adherence with College policies.

They must follow the reporting procedures where they are worried, concerned or where they believe an Online Safety incident has taken place involving them or another member of the College community. Any breach by

a student of this policy will be dealt with via the Student Positive Engagement Policy and Procedure.

4.3 Staff

All staff are expected to be vigilant with regard to Online Safety and complete their 'Essential for all' general awareness raising Online Safety development as part of their professional development.

Teaching staff and Tutor Mentors are expected to teach, guide and support students to develop Online Safety skills, providing a model example to students through embedded good practice with regard to topics including, though not limited to, cyber-bullying, sexting, online grooming, and malicious 3rd party applications.

Digital communication with students must be professional at all times and in the main restricted to College systems/networks (Microsoft Outlook email, ProMonitor, ProPortal, Google Apps for Education, Txttools, Moodle).

Teaching staff are encouraged to utilise technology to aid their teaching and working practices. They are responsible for ensuring the high standards of professionalism laid out in this policy and its associated acceptable use policies are still maintained through weekly moderation.

External platforms not hosted by the College such as social media sites should not be used for individual friendships with students except in exceptional circumstances where a pre-existing relationship already exists. Any breach by a member of staff of this policy that brings the College into disrepute will be dealt with via the Staff Disciplinary Policy and Procedure.

5 Security

The College will do all it can to make sure the College network is safe and secure. Every effort will be made to keep security software up to date. Appropriate security measures include the use of web and spam filtering, anti-virus/malware scanning, access controls, and firewalling, to prevent accidental or malicious access of college systems and information.

The College's Marketing Department undertakes a combination of manual and automated (via Vuelio media monitoring service) monitoring of social media sites and blogs. Whilst the college can monitor these sites, it cannot be responsible for the security of external online platforms. Staff and students have a responsibility to keep themselves safe when using these. However when it comes to the College's attention that abuse has occurred, for example, cyber-bullying, the College will take action.

The College monitors and records web activity from devices using the College's internet connection. Inappropriate activity is flagged to the College's Safeguarding team. This is in the form of real-time email alerts and scheduled daily, weekly, and monthly activity reports. The Safeguarding team will take action where they believe there is a significant risk of harm to the individual concerned or to others.

6 Risk Assessment

The College has conducted self-assessment risk assessments in all of its emerging technology use, providing opportunities to create staff guidance documents via a Bring Your Own Device (BYOD) Acceptable Use Policy, Use of Photos, Videos and Media Acceptable Use Policy, and Cloud Computing Acceptable Use Policy.

Staff should encourage students to use the World Wide Web and emerging technologies. However in doing so, care should be taken to judge the digital literacy of the students and their ability to keep themselves safe. Again, the acceptable use policies will be shared and disseminated to the student body.

7 Behaviour

The Sheffield College will ensure all users of technologies adhere to the standard of behaviour as set out in the ICT Facilities Access Regulations (IFAR) user agreement. The College will not tolerate any abuse of IT systems. Whether offline or online, communications by staff and learners should be courteous and respectful at all times.

Any reported incident of bullying, harassment or other unacceptable conduct will be treated seriously and in line with the Student Positive Engagement Policy and Disciplinary Procedure and the Staff Disciplinary Policy and Procedure.

When conduct is found to be unacceptable, the College will deal with the matter internally. Where conduct is considered illegal, the College will report the matter to the Police. Where a designated Safeguarding Officer judge's abuse has occurred, or there is a potential for significant abuse to occur, actions detailed in the Safeguarding Policy and Procedures will be taken.

8 Use of Images, Video and personal Information

The use of images or photographs is popular in teaching and learning. This is encouraged where there is no breach copyright or other rights of another person, for example, image rights or rights associated with personal data. This includes images downloaded from the internet and those belonging to staff or learners. Most images and photos are likely to be protected by copyright and this means that a user will need the permission of the copyright owner(s) if they want to copy the image or share it on the internet.

Specific information on UK copyright requirements provided by the Intellectual Property Office may be accessed here. Photos or videos of students for assessment of publicity purposes must conform to the Use of Photos, Videos and Media Acceptable Use Policy.

9 Education and Training

With the current unlimited nature of internet access it is impossible for the College to eliminate all risks for staff and students. It is our view therefore that the College should support staff and learners to stay safe online through proactive training and education so that individuals develop the necessary skills to be able to identify risks independently and manage them effectively. To this end, online general awareness raising training has been compiled for Online Safety and is mandated to all staff. Topics within this training include: awareness raising on cyber-bullying, cyber-grooming, cyber-stalking and personal online security. Awareness and skills training for students is delivered through a variety of ways, details of which are in the self-assessment in Appendix 1.

10 Incidents and Response

When an Online Safety incident is reported to the College this matter will be dealt with very seriously. The College will act immediately to prevent, as far as reasonably possible, any harm or further harm occurring.

If a student wishes to report an incident, they can do so in confidence via safeguarding@sheffcol.ac.uk, to their Tutor Mentor or directly to either the College's Lead Safeguarding Officer, Caroline Morrison, caroline.morrison@sheffcol.ac.uk or the IT Manager, Martin Plummer, martin.plummer@sheffcol.ac.uk.

Where a member of staff wishes to report an incident, they must contact their Line Manager or the College's Online Safety Coordinators as soon as possible. Alternatively they may also use the safeguarding@sheffcol.ac.uk link.

Following any incident, the College will review what has happened and decide on the most appropriate and proportionate course of action. Sanctions may be put in place, external agencies may be involved or the matter may be resolved internally depending on the seriousness of the incident. Serious incidents will be dealt with by Senior Management, in consultation with appropriate external agencies.

11 Feedback and Further Information

The Sheffield College welcomes all constructive feedback on this and any other College policy to provide clearer direction and support. We will always consult with staff and students regarding any major revision of the Online Safety Policy.

If you would like further information on Online Safety or wish to send us your comments on our Online Safety Policy then please contact our Online Safety Coordinators, Caroline Morrison and Martin Plummer.