E-Safety Policy, Guidelines and Procedures

Owning Strategy: Safeguarding Strategy	**Related Strategies:** IT Strategy
Relevant to: All Sheffield College Employees and Students	

Office Use only:

Corporate Intranet Family:	Approval Board/ Committee/Group:	Approval/ Re-approval Date:	Implementation Date:	Next Review Date:
	Safeguarding Strategic Board Executive Owner: Deputy Chief Executive and Deputy Principal	September 2022	September 2022	May 2023

New Policy or Substantive Policy Review

Version	Date	Policy Development Agreed by	Policy Development Author	Draft Policy Verified by	Policy Approval
V1	September 2020	Deputy Chief Executive	Assistant Principal Student Experience	Safeguarding Strategic Board	Safeguarding Strategic Board

Rationale for new or substantive policy review	

Please make explicit if change/review relates to procedures, guidelines and associated documents only

Periodic Policy Review / Change History

Version	Date of Review / Revision	Description of Change	Reviewed By	Approved By
V2	July 2021	- Update of Job titles throughout the document - Pg 5 replace IT teams with Head of IT and Development - Replaced "ICT" with "digital technologies" through the document	Head of Safeguarding and EDI	Safeguarding Strategic Board
V3	July 2022	- Update of Job titles throughout the document - Pg 2 – Home Working Policy added as a linked document. - Pg 7 – information added regarding the Ripple Software monitoring system. - Appendix 1 added – Ripple Software guidance for students at enrolment. - Pg 10 – paragraph on switching off web filtering changed from Chief Exec to Strategic Safeguarding Board. - Pg 15 – Web Filtering to be added as a standing agenda item for the Strategic Safeguarding Board	Head of Safeguarding and EDI	Safeguarding Strategic Board

Announcement on hub ☑
College newsletter □
SLT meeting □
External website ☑

SLT email ☑
All staff email □
Cascade brief ☑
Training needed (specify who) □

1. Policy Statement

New technologies have become integral to the lives of employees and students in today's society, both within College and in their lives outside College.

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

The requirement to ensure that all 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 Colleges are bound. This is also reflected in the Byron Review, which identified that alongside new technology a new culture of responsibility was needed, where all in society focus not on defending well-established positions, but on working together to help young people keep themselves safe, to help parents/guardians to keep them safe and to help each other support young people and parents/guardians in this task.

The policy forms part of the College's protection from legal challenge, relating to the use of Information and Communication Technology (ICT). Many of the risks reflect situations in the off-line world and it is essential that this policy is used in conjunction with other College policies.

2. Definitions

E-Safety is defined as the awareness, practice, and training of individuals together with IT infrastructure security and integrity to ensure the safe use of online technologies, thus maintaining both an individual's physical and psychological wellbeing as well as organisational reputation.

3. Principles

This policy and related procedure and guidelines have been produced as a framework for the protection of all in relation to e-Safety.

The education of students in e-Safety is an essential part of the College's e-Safety provision. Students need the help and support of the College to recognise and avoid e-Safety risks and build their resilience.

E-Safety awareness will be provided by the College in a variety of ways, including tutorial and online support.

Many parents and carers have only a limited understanding of e-Safety risks and issues, yet they play an essential role in the education of their dependents and in the monitoring/regulation of their on-line experiences.

4. Scope and Limitations

This policy applies to all employees, students, and visitors to Sheffield College who have access to and are users of College IT systems, both in and out of college.

The Education and Inspections Act 2006 empowers the Chief Executive, to such an extent as is reasonable, to regulate the behaviour of students when they are off the College site and empowers College employees to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other e-safety incidents covered by this policy, which may take place out of college, but is linked to membership of the College.

The College will deal with such incidents within this policy and related policies and will, where known, inform parents/carers and/or external agencies of incidents of inappropriate e-safety behaviour that takes place out of college.

5. Responsibilities

The Vice Principal for Student Experience is responsible for overseeing the implementation of the arrangements covered by this policy.

The Head of Safeguarding and EDI with the Head of IT are responsible for the development of the policy.

The Heads of Student Experience or agreed equivalent where there is no Head of Student Experience post, are responsible for the implementation of this policy within their faculty.

The roles and responsibilities of employees in implementation of this policy are clearly identified within the Procedures section.

6. Implementation Arrangements

All new employees are made aware of the policy and procedures during the formal employee induction process.

Updated and amended procedures are discussed in training sessions, team meetings and via email communications as appropriate. And this policy is available via the college website.

7. Monitoring and Review

The Head of IT will be responsible for monitoring the effectiveness of the policy.

Any serious weakness will be reported to the Safeguarding Strategic Board, who have the responsibility of ensuring the overall effectiveness of the policy.

Due to the ever-changing nature of Information and Communication Technologies, the e-Safety Policy will be reviewed annually and, if necessary, more frequently in response to any significant new developments in the use of the technologies, new threats to e-Safety, organisational or management changes or incidents that have taken place.

8. Related Documents

- Safeguarding Policy
- Information Technology Employee Acceptable Use Policy
- Student Positive Engagement & Behaviour policy
- Disciplinary Policy for Staff
- Data Protection Policy
- Social Media Policy
- IT Security Policy
- Information Technology Student Acceptable Use Policy
- Home Working Policy
- IT Strategy
- Due Diligence Checks – Virtual Experience of Work Guidance

GUIDELINES

The use of exciting and innovative tools in college and at home has been shown to raise educational standards and promote student achievement. However, the use of these technologies can put young people at risk within and outside College. 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 risks posed could be in the context of criminal and/or sexual exploitation, radicalisation, extremism, or extortion
- 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

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential to build student and employee 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 development and expansion of the use of digital technologies, and particularly of the internet, has transformed learning in recent years. Students need to develop high level digital skills, not only to maximise their potential use as a learning tool, but also to prepare themselves as lifelong students and for future employment. There is a large body of evidence that recognises the benefits that digital technologies can bring to teaching and learning. Sheffield College has made a significant investment both financially and physically to ensure these technologies are available to all students. The benefits are perceived to "outweigh the risks."

However, the College must, through its e-Safety policy, ensure that they meet their statutory obligations to ensure that employees and students are safe and are protected from potential harm, both within and outside College.

Technical – Infrastructure/Equipment, Filtering and Monitoring

The College will be responsible for ensuring that the College infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their e-Safety responsibilities.

- College IT systems will be managed in ways that ensure that the College meets e-Safety technical requirements
- There will be regular reviews and audits of the safety and security of College IT systems
- IT systems and equipment are secured appropriately, in line with the College IT Security Policy
- All users will have clearly defined access rights to College IT systems. Details of the access

rights available to groups of users will be recorded by the IT Team.

- All users will be provided with a username and password by the Head of IT who will keep an up-to-date record of users and their usernames
- 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 evident that there has been a breach of security
- Where necessary monitoring takes place in line with college policy
- College IT technical staff may monitor and record the activity of users on the College IT systems and users are made aware of this in the Acceptable User Policy
- An appropriate system is in place for users to report any actual/potential e-Safety incidents in line with the College's Safeguarding Policy
- Guidelines are in place regarding the extent of personal use that users are allowed on laptops and other portable devices that may be used out of college
- Guidelines are in place that control what software staff can install on college workstations / portable devices
- The College infrastructure and individual workstations are protected by up-to-date virus software
- Personal data should not be sent over the internet or taken off the College site unless safely encrypted or otherwise secured.
- From September 2022, the College will be implementing a new software designed to monitor searches online in relation to suicidal ideation. Where students or staff search information relating to suicide etc. A pop-up will appear on their search engine offering support for suicidal ideation.
- It is recognised that this may impact some curriculum areas such as, Health and Social Care, and therefore the Head of IT and the Head of Safeguarding & EDI worked closely together with curriculum to ensure that curriculum teams are fully prepared for the implementation.
- It is further recognised that the pop-up may cause an emotional reaction in both students and staff. Therefore, communications will be sent to all staff prior to the launch of the software. The Head of Safeguarding has also developed an information pamphlet for students at enrolment to ensure that they are aware. This is **Appendix 1** to this document.

Curriculum Focus

- E-safety should be a focus in all areas of the curriculum and employees should reinforce e-Safety messages in the use of IT across the curriculum and via tutorials and enrichment activities
- In lessons where internet use is pre-planned, it is best practice that students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- Where students are allowed to freely search the internet, e.g., using search engines, employees should be vigilant (as far as possible) in monitoring the content of the websites the student visits
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g., racism, drugs, and discrimination) that would normally result in internet searches being blocked. In such a situation, employees can request that the Head of IT can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need. Such requests must be made via the Faculty Head of the area
- Students should be taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information

- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet

Use of Digital and Video Images - Photographic, Video

- The development of digital imaging technologies has created significant benefits to learning, allowing employees and students instant use of images that they have recorded themselves or downloaded from the internet. However, employees and students 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. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees. The College will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm.
- When using digital images, employees should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. They should recognise the risks attached to publishing their own images on the internet, e.g., on social networking sites
- Employees are allowed to take digital / video images to support education aims, but must follow College policies concerning the sharing, distribution, and publication of those images. Those images should only be taken on college equipment. The personal equipment of employees should not be used for such purposes
- Care should be taken when taking digital / video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the College into disrepute
- Students must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images
- Students' full names will only be used where their or their parents/guardians written consent has been sought (where necessary) for use on a website or blog, particularly in association with photographs
- Where necessary written permission from parents/guardians will be obtained before photographs of students are published on the College website
- Students' work can only be published with the permission of the student and parents/guardians, where necessary

Data Protection

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

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection

Information on how the College adheres to these principles can be found in the Privacy Policy.

Following several “high profile” losses of personal data by public organisations, colleges are likely to be subject to greater scrutiny in their care and use of personal data. Please also refer to the College’s Data Protection Policy for further information.

Communications

A wide range of rapidly developing mobile communications technologies has the potential to enhance learning. Guidelines for use of mobile communication technologies identifies how the College currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:

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

- When on College premises the official College email service may be regarded as safe and secure and is monitored. Employees and students should therefore only use the College email service to communicate with others when in college, or on college systems (e.g., by remote access)
- Users need to be aware that email communications may be monitored
- Users must immediately report to their line manager/personal coach 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 employees and students or parents / guardians (email, chat, Google Classroom etc.) must be professional in tone and content. These communications may only take place on official College systems that fall under the Acceptable User Policy. Personal email addresses, text messaging or public chat / social networking programmes must not be used for these communications. The exception being Linkedin.com in relation to career development activities
- Students should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material
- Personal information should not be posted on the College website and only official email addresses should be used to identify employees
- Personal mobile telephone numbers must not be released to students

Unsuitable / Inappropriate Activities

Some internet activity e.g., accessing child abuse images or distributing racist material is illegal and would obviously be banned from college and all other IT systems. Other activities e.g., Cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a college context, either because of the age of the users or the nature of those activities.

Sheffield College believes that the activities referred to in the Acceptable User Policy would be inappropriate in a college context and that users should not engage in these activities in College or outside College when using College equipment or systems. The College policy restricts certain internet usage also.

Responding to Incidents of Misuse

It is hoped that all members of the College community will be responsible users of digital technologies, who understand and follow this policy, procedures, and guidelines. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse:

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

In the case of the disclosure of a safeguarding issue the Safeguarding Policy should be consulted, and actions followed in line with the flow chart, in particular the sections on reporting the incident to the police and the preservation of evidence.

If employees suspect that misuse might have taken place, but that the misuse is not illegal it is essential that correct procedures are used to investigate, preserve evidence, and protect those carrying out the investigation.

If anyone suspects that an individual is accessing an illegal website this should not be accessed by the individual themselves but reported in line with the College's Safeguarding Policy.

It is more likely that the College 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 College community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through college behaviour/disciplinary procedures.

Web Filtering

- The College maintains and supports the managed filtering service provided by the managed web filtering service.
- In the event of the Head of IT (or nominated deputy) needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Strategic Safeguarding Board.
- Requests from employees for sites to be removed from the filtered list will be considered by the Head of IT. Such requests must be made via the Assistant Principal, or equivalent, of the area, as appropriate.

Computer Network Acceptable User - Staff

General Principles

- The use of college provided network systems and services, including but not limited to, Internet, intranet, email, and SMS services, will be monitored for unusual activity and for reasons of security and/or network management. Users may also be subject to limitations on their use of such resources.

- Correspondence via email or other electronic means cannot be guaranteed to be private. Any confidential email should be sent using only encryption techniques sanctioned by the College.
- The distribution of any information through the Internet, computer-based services, email and messaging systems is subject to scrutiny. The College reserves the right to determine the suitability of this information. Limited personal use of the Internet and email services is permitted for skills development but is subject to the terms laid out below.

Conditions of Use

Users shall not:

- Visit Internet sites that contain obscene, hateful, or other objectionable materials as defined in the Internet Site Criteria document; send or receive by electronic means material that is obscene or defamatory or which is intended to annoy, harass, or intimidate another person. This includes, but is limited to, the following.

  - ➢ Child sexual abuse images
  - ➢ Promotion or conduct of illegal acts, e.g., 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
  - ➢ 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 College or brings the College into disrepute

- Solicit non-College business for personal gain or profit
- Use the Internet, email, telephone system or SMS service for any illegal purpose
- Use systems, applications, websites, or other mechanisms that bypass the filtering or other safeguards employed by the College
- Represent opinions as those of the College
- Make or post indecent remarks, proposals, or materials
- Upload, download or otherwise transmit commercial software or any copyrighted materials belonging either to parties outside of the College or to the College itself
- Install or run any unauthorised software on college equipment
- Download any software or electronic files without implementing virus protection measures that have been approved by the College
- Intentionally interfere with the normal operation of the network, including, but not limited to, propagation of computer viruses and sustained high volume network traffic which substantially hinders other users in their use of the network
- Use Internet, email or SMS services for inappropriate personal use that is not connected with college business
- Reveal or publicise confidential or proprietary information which includes, but is not limited to financial information, new business ideas, marketing strategies and plans, databases and information contained therein, student enrolment details and business relationships

- Transfer or upload personal data, as defined by the Data Protection Act 1998, onto any device, equipment or system not owned by the College without the express permission of the Head of IT and Development.

- Transfer personal data, as defined under the GDPR Act, onto any portable storage device, e.g., USB key stick, even if the device is owned by the College without the express permission of the Head of IT.
- Examine, change or use another users' files, output or user name for which they do not have explicit authorisation
- Reveal individual passwords, either account logon or system specific, to anyone else
- Resell any service provided by the College, including but not limited to email, network storage and Internet access
- Perform any other inappropriate uses identified by the Head of IT.

Users who violate any of the procedures/guidelines set in the policy may be subject to disciplinary action. The College also retains the right to report any illegal activities to the appropriate authorities.

The use of Mobile Communication Technologies

The table below outlines the use of mobile communication technologies for employees and students within Sheffield College.

	Employees					Students			
Communication Technologies	Allowed	Allowed with limitations	Allowed at certain times	Allowed for selected employees	Not allowed	Allowed	Allowed at certain times	Allowed with employees permission	Not allowed
Mobile phones may be brought to college	🟩					🟩			
Use of mobile phones in lessons			🟩					🟩	
Use of mobile phones in social time	🟩					🟩			
The use of college devices to take photos on mobile phones or other camera devices			🟩					🟩	
Use of handheld devices e.g. PDAs, PSPs	🟩						🟩		

Procedure

The following procedure details the roles and responsibilities for e-safety of individuals and groups within Sheffield College.

Chief Executive and Principal

The Chief Executive and Principal has overall responsibility for all matters relating to safety, including e-Safety. This responsibility includes ensuring that management is addressed through comprehensive policies and procedures that are effectively implemented and appropriately resourced within the overall financial position of the College.

In addition, each member of the Governing Body has an individual role in providing leadership and ensuring that all decisions reflect the intentions outlined in this policy.

College Leadership Team

Members of the College Leadership Team are responsible for ensuring that this policy is understood by all employees and fully implemented within their area(s) of responsibility. They are responsible for ensuring that within their areas there are effective arrangements in place for the prompt reporting and management of any adverse incidents.

Head of Safeguarding and EDI

The Head of Safeguarding and EDI is responsible for:

- Producing and reviewing the College's e-Safety Policy and supporting documents, in liaison with the Head of IT and Development.
- Ensuring that there are procedures in place that need to be followed in the event of an e-Safety incident taking place and that these are communicated.
- Ensuring that appropriate training and advice for employees and students is available.
- Receiving reports of e-Safety incidents and creating a log of incidents to inform future e-Safety developments.

Head of IT and Development

The Head of IT and Development is responsible for ensuring:

- That the College's IT infrastructure is secure and is not open to misuse or malicious attack
- That the College meets the e-Safety technical requirements outlined in the Acceptable use policy
- That users may only access the College's networks via password protection
- The College's web filtering policy is applied and updated on a regular basis
- That the College keeps up to date with e-Safety technical information to effectively carry out its e-Safety role and to inform and update others as relevant
- That any concerns raised over the use of the network/Virtual Learning Environment (Google Classroom)/remote access/email will be investigated in accordance with college policy
- That monitoring software/systems are implemented and updated as agreed, in line with college policies

Head of Tutorial and Student Progress

- Is responsible for ensuring that e-Safety education is delivered effectively to students via enrichment and tutorial activities.

Employees

Employees are responsible for ensuring that:

- They have an up-to-date awareness of e-Safety matters and of the current College e-Safety Policy and supporting documents
- They have read, and understood the College Employee Acceptable User Policy/Agreement
- They report any suspected misuse or problem to the appropriate person, in line with College Policy
- Digital communications with students (email/Virtual Learning Environment (VLE)/voice) should be on a professional level and only carried out using official College systems
- E-Safety issues are embedded in aspects of the curriculum and other College activities
- Students understand and follow the College e-Safety and Acceptable User Policy
- Students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- They monitor the use of digital technologies in lessons, extra-curricular and extended College activities
- They are aware of e-Safety issues related to the use of mobile phones, cameras and handheld devices and that they monitor their use and implement current College policies with regard to these devices.
- In lessons where internet use is pre-planned students are guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Designated Safeguarding Lead

The Designated Safeguarding Lead has day-to-day responsibility for e-Safety, and should be aware of the potential for serious safeguarding issues arising from:

- Sharing of personal data
- Access to illegal / inappropriate materials
- Inappropriate on-line contact with adults / strangers
- Potential or actual incidents of grooming
- Cyber-bullying

Students

- Are responsible for using the College IT systems in accordance with the Student Acceptable User Policy, which they will be expected to sign before being given access to college systems
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations

- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- Will be expected to know and understand College policies on the use of mobile phones, digital cameras, and handheld devices. They should also know and understand College policies on the taking / use of images and on cyber-bullying

- Should understand the importance of adopting good e-Safety practice when using digital technologies out of college and realise that the College's e-Safety Policy covers their actions out of College, if related to their membership of the College

Organisational Arrangements - Safeguarding Strategic Board

The Safeguarding Strategic Board is responsible for the endorsement, approval and implementation of all safeguarding related policies.

A key function of the group is to establish and maintain standards of e-Safety by developing and monitoring College e-Safety policies and procedures. The group aims to promote a culture of understanding and co-operation across the College to ensure the safety of all.

A standing agenda item for the Strategic Safeguarding Board will be Web Filtering, specifically, where staff or students have made requests for certain internet searches/websites etc. To be exempt from being blocked, members of the Strategic Safeguarding Board will discuss at each meeting and agree whether the request can be authorised.