IT & Communication Systems Policy

Date updated:

January 2023

Date to Governors:

Compliance Lead:

Assistant Principal

Date for Review:

January 2025

Policies & Procedures

Contents

1. Aim

1.1 This policy describes how Rotherham Opportunities College (ROC) will comply with Data Protection Act 2018 in delivering the functions of the organisation through Information Technology and Communication (ICT) Systems.

1.2 The policy is split into 3 categories:

- E-safety and Social Media
- Information and Cyber Security
- Trusted Websites and Monitoring

2. Definitions

Term	Definition
E-Safety	Ability to protect and educate students and staff in their use of technology online.
Social Media	**Social media** is an online function where people and organisations connect, share information and communicate with each other.
Information and Cyber Security	Information Security The protection of information and **information** systems from unauthorized access. Cyber Security The protection of networks, computers from unauthorised electronic access.
Trusted Websites	A **trusted** site is a website that you trust not to damage your computer/information systems
ICT and ICT systems	ICT refers to technologies that provide access to information through telecommunications.
Application Software	Include such things as database programs, word processors, Web browsers and spreadsheets.

3. Roles and responsibilities

3.1 This policy relies on management and user actions to ensure that its aim is achieved. Any breach of this policy will instigate disciplinary action. Consequently, roles and responsibilities are defined below.

3.2 The Directors and Governing Body of ROC.

The Directors and Governing Body of ROC have ultimate corporate responsibility for ensuring that the college complies with this policy.

3.3 The CEO and Principal of ROC

The CEO and principal are responsible for ensuring that the policy requirements relating to the use of ICT systems are met including the responsibility for ensuring that users of systems and data are familiar with all aspects of this policy.

3.4 Specialist Roles (E-Safety including Social Media, IT/Security and Data Protection)

The college will have named specialist leads who are responsible for overseeing the implementation of relevant aspects of this policy, monitoring compliance and recommending related policies and guidelines where applicable.

The college will ensure that lead officers are trained appropriately and contact details are communicated to all users of Rotherham Opportunities College's ICT systems.

3.5 Information Asset/System Owners

The college will have Information Asset/System Owners (IAOs) who are senior responsible individuals involved in running the relevant business and together form the Senior Information Risk Owner (SIRO) team. Their role is to understand and address risks to information and recommend appropriate improvements in the use of ICT systems where applicable. The College Data Protection Officer is Louise Smith (Assistant Principal) and the college use GDPRiS as a risk management tool for information management.

3.6 All Users

3.6.1. Users are those employees, students or authorised guests of Rotherham Opportunities College who make use of ICT systems to support them in their work.
All users of ROC's ICT systems and data must comply with the requirements of this policy.
The policy has an Acceptable Use Agreement which summarises the responsibilities of users.
3.6.2. Users are responsible for notifying the principal of any breach of policy.
3.6.3. Users are responsible for the security of applications and equipment they use.

4. E-Safety Policy

4.1 Purpose

Rotherham Opportunities College seeks to ensure that internet, mobile and digital technologies are used effectively, for their intended educational purpose, in ways that will not infringe legal requirements or create unnecessary risk.

The college expects everyone to use internet, mobile and digital technologies responsibly and strictly according to the conditions set out in this policy. This policy also includes expectations on appropriate online behaviour and use of technology outside of the college for students, parents/carers, staff and governors/ directors and all other visitors to Rotherham Opportunities College.

4.2 Use of email

Staff and governors/ directors should use a Rotherham Opportunities College email account for all official communication to ensure everyone is protected through the traceability of communication. Under no circumstances should staff contact students, parents/carers or conduct any college business using a personal email address.

Students may only use college approved accounts on ROC's systems and only for educational purposes.

For advice on emailing, sharing personal or confidential information or the need to gain parent/carer permission refer to the organisations Data Protection Policy and or the organisations data protection lead officer.

Emails created or received as part of college business will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000.

Staff, governors/ directors and students should not open emails or attachments from suspect sources and should report their receipt to the IT/security lead officer.

Users must not send emails which are offensive, embarrassing or upsetting to the college or to anyone (i.e. cyberbullying).

4.3 Visiting online sites and downloading

- Staff must preview sites, software and apps before their use in ROC business or before recommending them to students. Before using any online service that requires user accounts to be created or the sharing of any personal data, staff must consult with the data protection lead officer with details of the site/service. If internet research is set for homework or remote learning, specific sites will be suggested that have previously been checked by the teacher. All users must observe copyright of materials from electronic sources.

- Staff must only use pre-approved systems if creating blogs, wikis or other online areas in order to communicate with students/ families.

- When working with students searching for images should be done through Google Safe Search, Google Advanced Search or a similar application that provides greater safety than a standard search engine.

Users must not:

Visit internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:

- Indecent images of children actually or apparently under the age of 18 or images of child abuse (i.e. images of children, digital or cartoons, involved in sexual activity or posed to be sexually provocative);
- Indecent images of vulnerable people over the age of 18 (i.e. images of vulnerable people, digital or cartoons involved in sexual activity or posed to be sexually provocative);
- Adult material that breaches the Obscene Publications Act in the UK;
- Promoting discrimination of any kind in relation to the protected characteristics: gender identity and reassignment, gender/sex, pregnancy and maternity, race, religion, sexual orientation, age and marital status;
- Promoting hatred against any individual or group from the protected characteristics above;
- Promoting illegal acts including physical or sexual abuse of children or adults, violence, bomb making, drug and alcohol abuse and software piracy;
- Any material that may bring the college or any individual within it into disrepute e.g. promotion of violence, gambling, libel and disrespect.

Users must not:

- Reveal or publicise confidential or proprietary information;
- Intentionally interfere with the normal operation of the networks and internet connection, including the propagation of computer viruses
- Transmit unsolicited commercial or advertising material either to other users, or to organisations connected to other networks except where permission has been given to the organisation;
- Use the college's systems and networks for running a private business;
- Intimidate, threaten or cause harm to others;
- Access or interfere in any way with other users' accounts;

- Use software or hardware that has been prohibited by the organisation.

Only a college device may be used to conduct ROC's business outside of the college. The only exception would be where a closed, monitorable system has been set up by the college for use on a personal device.

All breaches of prohibited behaviours detailed above will be investigated, where appropriate, in liaison with the police.

The college recognises that in certain planned curricular activities, access to controversial and/or offensive online content may be beneficial for educational use. In such circumstances, there is an expectation that access is pre-planned, risk assessed and recorded, and permission given by the principal.

4.4 Storage of Images

Photographs and videos provide valuable evidence of students' achievement and progress in a variety of contexts and can be used to celebrate the work of the college. In line with Data Protection Act 2018 they are used only with the written consent of the student and where appropriate parents/carers which is secured in the first instance on a student's entry to ROC. Records are kept on file and consent can be changed by students/parents/carers at any time.

Photographs and images of students are only stored on the college's agreed secure networks which include some cloud-based services. Rights of access to stored images are restricted to approved staff as determined by the Information Asset Owner. Staff and students may have temporary access to photographs taken during a class session, but these will be transferred/ deleted promptly.

There may be some students who are at risk and must not have their image posted online and others who do not want their image online. For these reasons, students/parents/carers must follow the college's Acceptable Use Agreement and refrain from taking or posting online photographs of any member of the college community, other than themselves (students) or their student/s (parents/carers).

Staff and other professionals employed by ROC who work with students, must only use college equipment to record images of students whether on or off site. Images of all staff who work at the college will be used in line with the college Staff Privacy Notice.

4.5 Use of personal mobile devices (including phones)

Rotherham Opportunities College allows staff, including temporary and peripatetic staff, and visitors to use personal mobile phones and devices only in designated areas and never in the presence of students. Under no circumstance does the college allow a member of staff to contact a student or parent/carer using their personal device unless the member of staff uses 3CX on their mobile device.

Parents/carers may only use personal mobile phones and devices in designated areas unless otherwise informed, e.g. for specific events and activities and they must only take photos or videos of their young person. These images are for personal use and the Data Protection Act does not apply. Under no circumstance should images be taken at any time on college premises or on off-site college events and activities of anyone other than their own young person. When a parent/carer is on college premises but not in a designated area, their phone/s must be kept out of sight and on silent mode.

Students are allowed to bring personal mobile devices/phones to college but must not use them for personal purposes within lesson time. In lesson times all such devices must be switched off and kept secure in the student's personal property e.g. bag or coat. Under no circumstance should students use their personal mobile devices/phones to take images of:

- any other student;
- any member of staff.

The college is not responsible for the loss, damage or theft on college premises of any personal mobile device.

Users bringing personal devices into college must ensure there is no inappropriate or illegal content on the device.

There are three main systems ROC permits to be used on personal devices as they are of major benefit to the running of the college and safeguarding of the students. These systems are stated below along with the main rules that accompany personal device usage in order to protect users and the personal data of everyone involved:

- CPOMS Safeguarding System
- Outlook
- 3CX

Guidelines applicable to all systems:
If staff have been issued with a business device this must always take priority for remote working use.
If a personal device is lost or stolen the staff member must immediately alert the college so appropriate security procedures can be initiated.
There is an expectation that due to the installation of these college applications that staff will have a secure PIN on their personal device. Staff must be mindful of personal data held within these applications and the risk associated such as unauthorised access if your personal device is shared with individuals such as family members.

Guidelines that are application specific:
3CX:
When on college business contact must always be made via the 3CX solution.
Ensure that parent/ carer/ student phone numbers are never stored in personal devices contact list.
Outlook:
ROC will only accept use of work emails via downloading the official Microsoft Outlook application from Microsoft Corporation.
CPOMS:
After each session that CPOMs is used on a personal device it must be logged out.

4.6 New technological devices

New personal technological devices may offer opportunities for teaching and learning.

However, the college must consider educational benefits and carry out risk assessment before use in college is allowed. Parents/carers, students and staff should not assume that new technological devices will be allowed in college and should check with the principal before they are brought into college.

4.7 Reporting incidents, abuse and inappropriate material

There may be occasions in college when either a student or a staff member receives an offensive, abusive or inappropriate message or accidentally accesses abusive material. When such a situation occurs the student or staff member must report the incident immediately to a member of the senior leadership team in college or the CEO or the safeguarding lead. Where such an incident may lead to significant harm, safeguarding procedures should be followed. The college takes the reporting of such incidents seriously and where judged necessary, the safeguarding lead will refer details to social care or the police.

4.8 Curriculum

Online safety is embedded within our curriculum. The college provides a comprehensive curriculum for safety which enables students to become informed, safe and responsible. This includes teaching to prevent radicalisation, for which staff provide a narrative to counter extremism.

The curriculum is flexible and can respond to any immediate online safety issues and risks as they emerge.

It is necessary for students to develop skills of critical awareness, digital resilience and good online citizenship to enable them to use internet, mobile and digital technologies safely and responsibly. Students are taught to recognise the creative, collaborative, cultural, economic and educational opportunities provided by the internet, mobile and digital technologies. Curriculum work will also include:

- Understanding how to use the internet, mobile and digital technologies in a balanced and appropriate way to avoid negative impact on wellbeing, e.g. regulated screen time and diverse online activity;

- Learning how to develop a positive online reputation and enhance future opportunities e.g. in relationships and employment;

- Developing critical thinking skills in relation to online content e.g. recognising fake news and extremism, understanding commercial manipulation, maintaining an authentic sense of self that is resilient to online pressure, learning how easy it is to lie online (i.e. users may not be who they say they are and may have ulterior motives);

- Understanding the dangers of giving out personal details online (e.g. full name, address, mobile/home phone numbers, college details, email address) and the importance of maintaining maximum privacy online;

- Thinking carefully before placing images online and considering their appropriateness and understanding the importance of gaining consent before posting photographs of others;

- Understanding the permanency of all online postings and conversations;
- Understanding relevant legislation, including copyright, and the importance of respecting other people's information, reputation and images;
- What constitutes cyberbullying, how to avoid it, the impact it has and how to access help.

5. Social Media Policy

5.1 Purpose

The widespread availability and use of social media applications bring opportunities to understand engage and communicate in new and exciting ways. It is important that we are able to use these technologies and services effectively and flexibly. However, it is also important to ensure that we balance this with our duties to our college, the community, our legal responsibilities and our reputation.

For example, our use of social networking applications has implications for our duty to safeguard children, young people and adults at risk.

The policy aims to provide this balance to support innovation whilst providing a framework of good practice which applies to all users of Rotherham Opportunities College's ICT systems.

The purpose of the policy is to:

- Protect the college from legal risks;
- Ensure that the reputation of the college, its staff and governors/ directors is protected;
- Safeguard all children, young people and adults at risk;
- Ensure that any users are clearly able to distinguish where information, provided via social media, is legitimately representative of the college.

All members of staff should bear in mind that information they share through social networking

applications, even if they are on private spaces, are still subject to copyright, data protection and freedom

of information legislation, the Safeguarding Vulnerable Groups Act 2006 and other legislation. They must also operate in line with the college's Equalities, Safeguarding and ICT Acceptable Use Agreements.

Within this policy there is a distinction between use of college sanctioned social medial for professional educational purposes, and personal use of social media.

5.2 Useof Social Media in practice

5.2.1 Personal use of social media

- College staff will not invite, accept or engage in communications with parents or students from the college community in any personal social media whilst in employment at Rotherham Opportunities College;
- Any communication received from students on any personal social media sites must be reported to the Designated Safeguarding Lead;
- If any member of staff is aware of any inappropriate communications involving any student in any social media, these must immediately be reported as above;
- Members of college staff are strongly advised to set all privacy settings to the highest possible levels on all personal social media accounts;
- All email communication between staff and members of the college community on college business must be made from an official college email account;
- Staff should not use personal email accounts or mobile phones to make contact with members of the college community on college business, nor should any such contact be accepted, except in circumstances given prior approval by the principal;
- Staff are advised to avoid posts or comments that refer to specific, individual matters related to the college and members of its community on any social media accounts;
- Staff are also advised to consider the reputation of the college in any posts or comments related to the college on any social media accounts;
- Staff should not accept any current student of any age or any ex- student of the college as a friend, follower subscriber or similar on any personal social media account.

5.2 2. College-sanctioned use of social media

There are many legitimate uses of social media within the curriculum and to support student learning. For example, the college has an official Twitter account, and several courses require the use of blogs for assessment. There are also many possibilities for using social media to enhance and develop students' learning.

When using social media for educational purposes, the following practices must be observed:

- Staff should set up a distinct and dedicated social media site or account for educational purposes. This should be entirely separate from any personal social media accounts held by that member of staff, and should be linked to an official college email account.
- The URL and identity of the site should be notified to the appropriate Information Asset Owner and/or principal before access is permitted for students;

- The content of any college sanctioned social media site should be solely professional and should reflect well on the college;
- Staff must not publish photographs of students without their written consent and if appropriate the consent of parents/carers;
- Staff must not identify by name any student featured in photographs, or allow personally identifying information to be published on college social media accounts unless the student has given their consent and where appropriate the consent of parents/carers;
- Care must be taken that any links to external sites from the account are appropriate and safe;
- Any inappropriate comments on or abuse of college sanctioned social media should immediately be removed and reported to the principal;
- Staff should not engage with any direct messaging of students through social media where the message
  is not public;

- All social media accounts created for educational purposes should include a link to the ICT Acceptable Use Agreement on the college website. This will indicate that the account is officially sanctioned by ROC.

6. Information and Cyber Security Policy

6.1 Purpose

The purpose of the policy is to ensure:

- information will be protected against unauthorised access;
- confidentiality of information will be assured;
- integrity of information will be maintained;
- regulatory and legislative requirements will be met;
- business continuity plans will be produced, maintained and tested;
- ICT security training will be available to all staff.

6.2 Physical Security

6.2.1 Location Access

- Adequate consideration should be given to the physical security of rooms containing ICT equipment (including associated cabling). As far as practicable, only authorised persons should be admitted to rooms that contain servers or provide access to data. The server rooms should be locked when left unattended. Ideally, such rooms should have a minimum of key pad access.
- The IT/Security lead must ensure appropriate arrangements are applied for the removal of any ICT equipment from its normal location. These arrangements should take into consideration the risks associated with the removal and the impact these risks might have.

6.2.2 Equipment siting

- Reasonable care must be taken in the siting of computer screens, keyboards, printers or other similar devices. Wherever possible, and depending upon the sensitivity of the data, users should observe the following precautions:
  - devices are positioned in such a way that information stored or being processed cannot be viewed by persons not authorised to know the information. Specific consideration should be given to the siting of devices on which confidential or sensitive information is processed or retrieved;
  - equipment is sited to avoid environmental damage from causes such as dust & heat;
  - users have been instructed to avoid leaving computers logged-on when unattended if unauthorised access to the data held can be gained. Clear written instructions to this effect should be given to users (in the acceptable use agreement);
  - users have been instructed not to leave hard copies of sensitive data unattended on desks.
- The same rules apply when accessing the college's ICT System or ICT data away from college, e.g. at a user's home or visiting another school or college.

6.2.3 Inventory

The Assistant Principal shall ensure that an inventory of all ICT equipment is maintained and all items accounted for at least annually.

6.3. Legitimate Use

The college's ICT facilities must not be used in any way that breaks the law or breaches college standards.

Such breaches include, but are not limited to:

- making, distributing or using unlicensed software or data;
- making or sending threatening, offensive, or harassing messages;
- creating, possessing or distributing obscene material;
- unauthorised personal use of the college's computer facilities.

6.3.1 Private Hardware & Software

Dangers can occur from the use of unlicensed software and software infected with a computer virus. It is therefore vital that any private software permitted to be used on the college's equipment is acquired from a responsible source and is used strictly in accordance with the terms of the licence. The use of all private hardware for college purposes must be approved by the principal and recorded by the IT/security lead.

6.3.2 ICT Security Facilities

The college's ICT systems and data will be protected using appropriate security arrangements as set out in this policy.

In addition, consideration should also be given to including appropriate processing controls such as audit trails, input validation checks, control totals for output, reports on attempted unauthorised access, etc.

For new systems, it is recommended that such facilities be confirmed at the time of installing the system.

6.3.3 Authorisation

Only persons authorised by an Information Asset Owner and or principal are allowed to use the college's ICT systems. The user's manager will ensure the user is fully aware of the extent to which they may make use of the ICT System and ensure they understand the relevant policy requirements before accessing ROC's ICT systems and data.

The college's IT/security lead will maintain a register of all system users, access and permissions.

Failure to establish the limits of any authorisation may result in the college being unable to use the sanctions of the Computer Misuse Act 1990. Not only will it be difficult to demonstrate that a user has exceeded the authority given, it will also be difficult to show definitively who is authorised to use a computer system.

Access eligibility will be reviewed continually, including remote access for support. In particular the relevant access capability will be removed when a person leaves the employment of the college. In addition, access codes, user identification codes and authorisation rules will be reviewed whenever a user changes duties.

Failure to change access eligibility and passwords will leave the ICT systems vulnerable to misuse.

6.3.4. Passwords

The level of password control will be defined based on the value and sensitivity of the data involved, including the possible use of "time out" passwords where a terminal/PC is left unused for a defined period.

- Passwords for staff users
  - Encryption passwords MUST be a minimum of 8 characters, including a mix of letters (upper and lower case) and numbers.
  - Laptop/computer passwords will be changed regularly, reminders will be given automatically.
  - Passwords should be memorised and if written down MUST NOT be kept with the device in any form.
  - Passwords or screen saver protection should protect access to all ICT systems.
  - A password must be changed if it is affected by a suspected or actual breach of security or if there is a possibility that such a breach could occur, such as:
    - when a password holder leaves the college or is transferred to another post;
    - when a password may have become known to a person not entitled to know it.
  - The need to change one or more passwords will be determined by the risk of the security breach.
  - Users must not reveal their password to anyone.

6.3.5. Security of the network

Only devices approved by the principal should be permitted to be connected to the network, either through wired or wireless connectivity.

Where devices are connected to the network using wireless, the wireless network should be secure; as a minimum this should be done using WPA. Open Access Wireless Access Points must not be connected to the college's network.

Encryption is applied to wireless networks, encryption keys should be kept secure and changed at least termly.

Mobile devices may, with permission, connect to the network but in full compliance with the ICT policies and this permission may be withdrawn at any time.

6.3.6 Encryption

All devices that have access to data attached to the ICT System are fully encrypted Devices subject to encryption may include:

- Laptops
- PDAs
- Smartphones
- USB Pendrives/Memory cards
- Desktops

Where technology prevents the use of encryption (e.g. SD Memory Cards used in Digital Cameras), then any personal/confidential data should not be stored on these devices.

6.3.7 Filtering of the Internet

Access to the internet for students should be filtered using an approved system.

It is the responsibility of the IT/Security lead to monitor the effectiveness of filtering at the college and report issues to the DSL and principal.

Where breaches of internet filtering have occurred, the IT/Security lead should inform the DSL and principal and assess the risk of continued access.

6.3.8 Backups

In order to ensure that essential services and facilities are restored as quickly as possible following an ICT system failure, back-up copies of stored data will be taken at regular intervals and managed by the IT/Security lead.

Data essential for the day to day running and management of the college should be stored on the college's network.

Backups contain data that must be protected and should be clearly marked as to what they are and when they were taken. They should be stored away from the system to which they relate in a restricted access fireproof location, preferably off site.

Instructions for re-installing data or files from backup should be fully documented and security copies should be regularly tested to ensure that they enable the systems/relevant file to be re-loaded in cases of system failure.

6.3.9 Operating System Patching

The IT/Security lead will ensure that all machines defined as part of the ICT System are patched up to date according to those releases distributed by the manufacturers of the operating systems.

6.3.10 Virus Protection

The college will use appropriate Anti-virus software for all college ICT systems.

All users should take precautions to avoid malicious software that may destroy or corrupt data.

The college will ensure that every ICT user is aware that any device in the ICT system (PC, laptops, netbook, PDA, cash till) with a suspected or actual computer virus infection must be disconnected from the network and be reported immediately to the IT/Security lead who must take appropriate action, including removing the source of infection.

The governing body/ directors could be open to a legal action for negligence should a person suffer as a consequence of a computer virus on college equipment.

Any third-party laptops/mobile devices brought into college will only be allowed to connect to the guest network, which provides a staff-level filtered internet connection. Third parties are responsible for ensuring that their devices are kept up-to-date with the latest patches and anti-virus software and definitions.

The college will ensure that up-to-date anti-virus signatures are applied to all servers and that they are available for users to apply, or are automatically applied, to PCs or laptops.

6.3.11 Disposal of Waste

Disposal of waste ICT media such as print-outs, CD's and magnetic tape will be made with due regard to the sensitivity of the information they contain. For example, paper will be shredded if any confidential information from it could be derived.

The Data Protection Act 2018 requires that adequate mechanisms be used when disposing of personal data.

6.3.12 Disposal of Equipment

The Data Protection Act 2018 requires that any personal data held on a part of the ICT system subject to disposal to be destroyed.

Prior to the transfer or disposal of any ICT equipment the IT/Security lead must ensure that any personal data or software is obliterated from the machine if the recipient organisation is not authorised to receive the data. Where the recipient organisation is authorised to receive the data, they must be made aware of the existence of any personal data to enable the requirements of the Data Protection Act to be met. Normal write-off rules as stated in Financial Regulations apply. Any ICT equipment must be disposed of in accordance with WEEE regulations

It is important to ensure that any copies of the software remaining on a machine being relinquished are legitimate. Care should be taken to avoid infringing software and data copyright and licensing restrictions by supplying unlicensed copies of software inadvertently. The college should maintain a regularly updated asset register of licenses and should indicate when licenses have been transferred from one part of the ICT system to another.

6.3.13 Repair of Equipment

If a machine, or its permanent storage (usually a disk drive), is required to be repaired by a third party the significance of any data held must be considered. If data is particularly sensitive it must be removed from hard disks and stored on alternative encrypted media for subsequent reinstallation, if possible. The college will ensure that third parties are currently registered under the Data Protection Act 2018 as personnel authorised to see data and as such are bound by the same rules as college staff in relation to not divulging the data or making any unauthorised use of it.

6.4. Security Incidents

6.4.1 All suspected or actual breaches of ICT security shall be reported to the IT/Security lead or the principal in their absence, who should ensure a speedy and effective response to be made to an ICT security incident, including securing useable evidence of breaches and evidence of any weakness in existing security arrangements. They must also establish the operational or financial requirements to restore the ICT service quickly. In addition, if the breach poses a risk to personal information, the relevant information asset owner and data protection lead should also be made aware so that an investigation can be instigated.

6.4.2 The Audit Commission’s Survey of Computer Fraud and Abuse 1990 revealed that over 50% of incidents of ICT misuse are uncovered accidentally. It is, therefore, important that users are given positive encouragement to be vigilant towards any suspicious event relating to ICT use.

6.4.3 It should be recognised that the college and its officers may be open to a legal action for negligence if a person or organisation should suffer as a consequence of a breach of ICT security within the college where insufficient action had been taken to resolve the breach.

6.5 Personal Use

6.5.1 The college has devoted time and effort into developing the ICT Systems to assist you with your work. It is, however, recognised that there are times when you may want to use the Systems for non-work related purposes, and in recognising this need the college permits you to use the Systems for personal use.

6.5.2 You must not use the Systems for personal use during working hours. You must not allow personal use of systems to interfere with your day to day duties. Any non-job related use of the Systems during working hours may be subject to disciplinary action.

6.5.3 You must not use college software for personal use unless the terms of the licence permit this and you are responsible for checking the licensing position.

6.5.4 You must pay all costs associated with personal use at the college’s current rates e.g. cost of paper.

6.5.5 You are responsible for any non-business related file which is stored on your computer.

7. Trusted websites and Monitoring

7.1 Purpose

This policy describes how we will monitor the use of our ICT systems.

This policy specifies:

- Our approach to identifying trusted websites;
- Our approach to monitoring usage of ICT devices, services and software, including printer usage and electronic door access logs;
- Intercepting communications on our ICT systems;
- The information we gather during usage logging;
- How we control content inspection.

We reserve the right to monitor the use of our ICT services, and access any information stored on our ICT infrastructure, but will do so in ways that are consistent with relevant legislation and guidance provided by the office of the UK Information Commissioner.

We will undertake such monitoring to:

- Comply with our regulatory and statutory obligations including PREVENT;
- Assess compliance with our Information Security Policy and Acceptable Use Agreements;
- Prevent and detect unauthorised use or other threats to our ICT systems;
- Evaluate staff training;
- Monitor system performance.

Web filtering is intended to prevent college facilities (software, computers, networks and offices) from being used to access illegal material.

Web filtering is in line with the college's current IT & Communications Systems Policy, which inhibits the use of its IT and networks for accessing a much wider range of offensive material, as well as PREVENT related material.

Such monitoring may include email, internet, telephone, mobile telephone and electronic file storage usage. Such monitoring is not, in general, person specific but your personal data may be accessed as part of this policy, but only in ways that are consistent with relevant legislation and good corporate governance.

7.2 Web Monitoring, Filtering and Blocking

The prevention of inappropriate use of the internet is aided by the use of the web filtering software. This enables blocking of inappropriate websites. Due to the nature of certain technologies, for example the wireless network, stricter criteria will at times need to be applied, meaning where web filtering software cannot determine whether a website is appropriate or not, it will be blocked.

Staff requesting the unblocking of websites for legitimate business use must obtain consent from their line manager before contacting the IT/Security lead in college. In addition, should the website be deemed controversial, additional approval is required from the principal.

Web filtering software is used to protect staff, students and visitors from inappropriate content. It can also help to protect the computer systems, in conjunction with anti-virus software, from potential system threats such as malware and viruses. E-mail filtering is used to detect potential issues and protect from spam, malware, phishing attacks and other e-mail based attacks.

7.3 Privacy

Our policy aims to provide an appropriate balance between respecting your privacy, whilst allowing the necessary monitoring required to meet our business needs and legal obligations.

7.4 Monitoring Definitions

This policy makes a distinction between:

- Usage logging: collecting data, usually from log files, about how and when a person uses our ICT systems;
- Content inspection: viewing information held within, for example, business or personal files or emails, or viewing of information on a VDU screen.

7.4.1 Usage Logging

We carry out 'usage logging' on a regular basis to ensure or improve the performance of our ICT services and to help identify and investigate potential prohibited use of our ICT systems (e.g. where a complaint or concern has been raised).

This is 'systematic monitoring' as defined by the Information Commissioner Office.

None of this data contains the content of the communication or the file – only information about the electronic activity.

7.4.2 Content Inspection

The college has the right to inspect the content in our ICT systems:

- To fulfil the college's business, when a user is unexpectedly absent or is on leave;
- To satisfy Data Protection subject access and Freedom of Information requests;
- Where we have reason to believe that a breach of our information security policy occurring, or has occurred (e.g. where a complaint or concern has been raised);
- At the request of law enforcement officers.

Content inspection involves viewing information contained within:

- Business files and documents;
- Printer usage and door access logs;
- Business-related email messages, telephone calls, videoconference sessions, chat sessions or any other ICT-based communications including internet usage logs;
- Business information displayed on a VDU screen.

If the system monitoring alerts us to a concern then a full investigation would be carried out at the request of the principal. An investigation would involve the interrogation of all college information systems.

7.5 Prohibited use

Where we have good reason to suspect that a member of staff is engaging in a prohibited use of our ICT systems – as set out in the ICT Acceptable Use Agreement – we may, in very exceptional circumstances, introduce covert monitoring of the individual.

We will only undertake such covert monitoring where there are strong grounds for suspecting criminal activity or equivalent malpractice, and where notifying an individual about the monitoring would prejudice its prevention or detection.

Covert monitoring will be strictly targeted at obtaining evidence within a set timeframe and will not continue after an investigation has been completed.

8. Training

All staff and governors/ directors are provided with ICT Systems training as part of their induction process.

ICT will also form part of continuing professional development, where changes to legislation, guidance or the college's processes make it necessary.

Students will receive guidance throughout the curriculum.

8.1 Acceptable Use Policy and Agreements

The college's Acceptable Use Policy and Agreements apply to all college staff, students and third parties who use ROC's ICT systems and or data to perform their work.

The policy covers the use of email, the internet, services accessed through the Internet and local file and network usage.

The conditions of use are explained in the policy and agreements. See appendices 1-3.

8.1.1 All college staff accessing these facilities must be issued with a copy of the 'Acceptable Use Policy' document, agreement and other relevant documents on induction.

For staff already employed within the college, retrospective agreement must be sourced.

A completed declaration will be required before access to ICT systems are granted. A copy of the completed agreement will be stored within the individuals personnel file.

8.1.2 All students attending the college must be supported to understand the 'Acceptable Use Policy' document where possible. The agreement form will be completed by students and, if appropriate, their parents. A completed declaration will be required before access to ICT systems are granted unless a bespoke situational assessment is made. A copy of the completed agreement will be stored within the individual student file.

8.1.3 In addition, copies of the 'Acceptable Use Policy' document and consent form will be issued to all visitors.

8.1.4 Any organisation working with students based on the college premises are also provided with a copy of the ICT System Policy and required to sign the Acceptable Use Agreement.

9. Monitoring and Review

The DPO on behalf of the Governing Body directors is responsible for monitoring and reviewing this policy. Review frequency has been set for every 2 years or prior at the request of the governing body/ directors.

10. Links with Other Policies

This IT and Communication Systems Policy is linked to our:

- Data Protection Policy
- Freedom of Information Policy
- Retention and Disposal Policy
- Data Breach Reporting Policy
- Safeguarding Adults Policy
- Safeguarding and Child Protection Policy

Appendix 1: Rotherham Opportunities College – Student Acceptable Use Agreement

My online safety rules

- I will only use college IT equipment for activities agreed by college staff.

- I will not use my personal email address or other personal accounts in college when doing college work.

- I will not sign up for any online service on college devices unless this is an agreed part of a college project approved by college staff.

- I will only open email attachments if it has been approved by a member of college staff.

- In college l I will only open or delete my files when told by a member of staff.

- I will not tell anyone other than my parents/carers my passwords. I will not use other people's usernames or passwords to pretend to be them online.

- I will make sure that all online contact I make is responsible, polite and sensible. I will be kind and respectful at all times.

- If I come across anything upsetting, unpleasant or nasty, or anything that makes me feel unsafe, I will tell my teacher or my parent/carer immediately.

- If someone says, asks or posts about me anything upsetting, unpleasant or nasty, or anything that makes me feel unsafe, I will not reply. I will tell a member of college staff or my parent/carer immediately.

- I will not give out my own or other people's personal information, including: name, phone number, home address, interests, college or clubs. I will tell a member of staff or parent/carer if anyone asks me online for personal information.

- Uploading or sending my image (photographs, videos, live streaming) online puts me at risk. I will not take, share or upload any image of anyone else without their permission and also, if they are a child, without their parent's/carer's permission.

- Even if I have permission, I will not upload any images, videos, sounds or words that **could** upset any member of the college community, now or in the future, as this is cyberbullying.

- I understand that some people on the internet are not who they say they are and some people are not safe to be in contact with. I will not arrange to meet someone I only know on the internet. If someone asks to meet me, I will not reply to them and I will tell a member of staff or a parent/carer immediately.

- I understand that everything I do or receive online can be traced now and in the future.

- I know it is important to build a good online reputation.
- I understand that some personal devices are allowed in college and some are not, and I will follow the rules. I will not assume that new devices can be brought into college without getting permission.
- I will not lie about my age in order to access games, apps or social networks that are for older people as this will put me at risk.
- I understand that these rules are designed to keep me safe now and in the future. If I break the rules staff will look into it and may need to take action.

Student's Name:

Signature:

Date:

Student agreement- To be recorded on Databridge and the signed copy to be added to the student's blue folder

Appendix 2: Rotherham Opportunities College – Staff and Governors Acceptable Use Agreement

You must read this agreement in conjunction with the ICT System policy and the Data Protection policy. Once you have read these, you must sign and submit this agreement and it will be kept on record in the college. You should retain your own copy for reference. This forms part of your professional and safeguarding responsibilities.

Internet, mobile and digital technologies are part of our daily working life and this agreement is designed to ensure that all staff and governors are aware of their responsibilities in relation to their use. All staff and governors are expected to adhere to this agreement and the relevant policy. Any concerns or clarification should be discussed with the principal. Breaches will be investigated, recorded and, where appropriate, disciplinary procedures will apply and police involvement will be sought.

Internet Access

I will not access or attempt to access any sites that contain any of the following: child abuse; pornography; discrimination of any kind; promotion of prejudice against any group; promotion of illegal acts; any other information which may be illegal or offensive. Inadvertent access on college equipment must be treated as an online safety incident, reported to the DSL in college and an incident report completed.

Online conduct

I will ensure that my online activity, both in and outside college, will not bring the college, my professional reputation, or that of others, into disrepute.

I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory. Exceptionally, use of controversial material as part of the curriculum should be planned and approved on every occasion (see policy).

I will report any accidental access to or receipt of inappropriate materials or filtering breach to the principal and/or Data Protection Lead.

I understand that all my use of the internet and other related technologies can be traced and monitored and, should it be required, must be made available to my line manager, principal and others as required.

I will not give out my personal contact and online account information such as phone numbers, email address, and social media account details to students and/or parents/carers (unless a bespoke arrangement has been made and sanctioned by the principal.)

Social networking

I understand the need to separate my professional role from my private friendships; in my professional capacity I will not become 'friends' with parents/carers or students on social networks. Where my college role is my only connection to an individual, private online contact is unacceptable with parents/carers or students.

When using social networking for personal use I will ensure my settings are not public. My private account postings will never undermine or disparage the college, its staff, governors, directors, parents/carers or students. Privileged information must remain confidential.

I will not upload any material about or references to the college or its community on my personal social networks unless in a capacity specifically requested or approved by the principal e.g. requests for raffle prizes for fetes etc.

Passwords

I understand that there is no occasion when a password should be shared with a student or a staff member.

Data protection

I will follow requirements for data protection as outlined in Data Protection policy. These include:

- Photographs must be kept securely and used appropriately, whether in college, taken off the college premises or accessed remotely;
- Personal data can only be taken out of college or accessed remotely when authorised by the principal or governing body;
- Personal or sensitive data taken off site must be encrypted.

Images and videos

I will only upload images or videos of staff, students or parents/carers onto college approved sites where specific permission has been granted or it is in line with the Staff Privacy Notice.

I will not take images, sound recordings or videos of college events or activities on any personal device. See section 4.5 linked to specific college systems.

Use of email

I will use my college email address for all college business. All such correspondence must be kept professional and is open to information requests under Data Protection and Freedom of Information legislation. I will not use my college email addresses for personal matters or non-college business.

Use of personal devices

I understand that as a member of college I should at no time put myself in a position where a safeguarding allegation can be made against me as a result of my use of personal devices. I understand that the use of personal devices in college is at the discretion of the principal.

I will only use approved personal devices in designated areas and never in front of students.

I will not access secure college information from personal devices unless a closed, monitorable system has been set up by the college.

Additional hardware/software

I will not install any hardware or software on college equipment without permission.

Promoting online safety

I understand that online safety is the responsibility of all staff and governors and I will promote positive online safety messages at all times including when setting homework or providing pastoral support.

I understand that it is my duty to support a whole college safeguarding approach and will report any inappropriate or concerning behaviour (of other staff, governors, visitors, students or parents/carers) to the principal.

Classroom management of internet access

I will pre-check for appropriateness all internet sites used in classrooms; this will include the acceptability of other material visible, however briefly, on the site. I will not free-surf the internet in front of students.

If I am using the internet to teach about controversial issues I will secure, on every occasion, approval in advance for the material I plan to use.

User signature

I agree to follow this Acceptable Use Agreement and to support online safety throughout the college. I understand this forms part of the terms and conditions set out in my contract of employment (staff members only) and/or my responsibilities as a governor/director.

Signature …….…………………….……………………………..………………

Date …………………………………….……

Full Name ………………………………………………………………..…….. (printed)

Job title ………………………………………………………………………………….………………….………………………………

<u>COPY FOR STAFF FILE</u>

Appendix 2: Rotherham Opportunities College – Staff and Governors Acceptable Use Agreement

You must read this agreement in conjunction with the ICT System policy and the Data Protection policy. Once you have read these, you must sign and submit this agreement and it will be kept on record in the college. You should retain your own copy for reference. This forms part of your professional and safeguarding responsibilities.

Internet, mobile and digital technologies are part of our daily working life and this agreement is designed to ensure that all staff and governors are aware of their responsibilities in relation to their use. All staff and governors are expected to adhere to this agreement and the relevant policy. Any concerns or clarification should be discussed with the principal. Breaches will be investigated, recorded and, where appropriate, disciplinary procedures will apply and police involvement will be sought.

Internet Access

I will not access or attempt to access any sites that contain any of the following: child abuse; pornography; discrimination of any kind; promotion of prejudice against any group; promotion of illegal acts; any other information which may be illegal or offensive. Inadvertent access on college equipment must be treated as an online safety incident, reported to the DSL in college and an incident report completed.

Online conduct

I will ensure that my online activity, both in and outside college, will not bring the college, my professional reputation, or that of others, into disrepute.

I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory. Exceptionally, use of controversial material as part of the curriculum should be planned and approved on every occasion (see policy).

I will report any accidental access to or receipt of inappropriate materials or filtering breach to the principal and/or Data Protection Lead.

I understand that all my use of the internet and other related technologies can be traced and monitored and, should it be required, must be made available to my line manager, principal and others as required.

I will not give out my personal contact and online account information such as phone numbers, email address, and social media account details to students and/or parents/carers (unless a bespoke arrangement has been made and sanctioned by the principal.)

Social networking

I understand the need to separate my professional role from my private friendships; in my professional capacity I will not become 'friends' with parents/carers or students on social networks. Where my college role is my only connection to an individual, private online contact is unacceptable with parents/carers or students.

When using social networking for personal use I will ensure my settings are not public. My private account postings will never undermine or disparage the college, its staff, governors, directors, parents/carers or students. Privileged information must remain confidential.

I will not upload any material about or references to the college or its community on my personal social networks unless in a capacity specifically requested or approved by the principal e.g. requests for raffle prizes for fetes etc.

Passwords

I understand that there is no occasion when a password should be shared with a student or a staff member.

Data protection

I will follow requirements for data protection as outlined in Data Protection policy. These include:

- Photographs must be kept securely and used appropriately, whether in college, taken off the college premises or accessed remotely;
- Personal data can only be taken out of college or accessed remotely when authorised by the principal or governing body;
- Personal or sensitive data taken off site must be encrypted.

Images and videos

I will only upload images or videos of staff, students or parents/carers onto college approved sites where specific permission has been granted or it is in line with the Staff Privacy Notice.

I will not take images, sound recordings or videos of college events or activities on any personal device. See section 4.5 linked to specific college systems.

Use of email

I will use my college email address for all college business. All such correspondence must be kept professional and is open to information requests under Data Protection and Freedom of Information legislation. I will not use my college email addresses for personal matters or non-college business.

Use of personal devices

I understand that as a member of college I should at no time put myself in a position where a safeguarding allegation can be made against me as a result of my use of personal devices. I understand that the use of personal devices in college is at the discretion of the principal.

I will only use approved personal devices in designated areas and never in front of students.

I will not access secure college information from personal devices unless a closed, monitorable system has been set up by the college.

Additional hardware/software

I will not install any hardware or software on college equipment without permission.

Promoting online safety

I understand that online safety is the responsibility of all staff and governors and I will promote positive online safety messages at all times including when setting homework or providing pastoral support.

I understand that it is my duty to support a whole college safeguarding approach and will report any inappropriate or concerning behaviour (of other staff, governors, visitors, students or parents/carers) to the principal.

Classroom management of internet access

I will pre-check for appropriateness all internet sites used in classrooms; this will include the acceptability of other material visible, however briefly, on the site. I will not free-surf the internet in front of students.

If I am using the internet to teach about controversial issues I will secure, on every occasion, approval in advance for the material I plan to use.

User signature

I agree to follow this Acceptable Use Agreement and to support online safety throughout the college. I understand this forms part of the terms and conditions set out in my contract of employment (staff members only) and/or my responsibilities as a governor/director.

Signature …….……………………….…………………………………..………………

Date ……………………………………….……

Full Name …………………………………………………………………..……... (printed)

Job title ……………………………………………………………………………………….………………….……………………………………

COPY FOR STAFF MEMBER

Appendix 3: Rotherham Opportunities College– Visitors, Volunteers and Parent Carer Helpers Acceptable Use Agreement

This document is designed to ensure that you are aware of your responsibilities when using any form of ICT in the college and other aspects of safeguarding in connection with online safety.

Please raise **any** safeguarding concerns arising from your visit immediately with the principal and/or the safeguarding lead.

- I understand I may only use my personal mobile phone(s) and other devices with camera functions in designated areas. When not in a designated area, phones must be switched off and out of sight. Any exception must be pre-arranged.
- I will not take images, sound recording or videos of college events or activities, on or off site, on any device. Any possible exception must be pre-arranged.
- I will not give out my personal details such as mobile phone number, email address, and social media account details to students and parent/carers. Where appropriate I may share my professional contact details with parents/carers provided the safeguarding lead or principal is informed before I leave the college.
- I understand my visit to the college may give me access to privileged information about students, staff, college systems and plans. Such information should never be shared specifically online, including on social media sites.
- I understand I should not use college equipment to access the internet without prior approval from my contact in the college or the principal.
- If working in the classroom, I will pre-check for appropriateness all internet sites I intend to use including checking the acceptability of other material visible on the site. I will not free-surf the internet in front of students. If I am in any doubt about the appropriateness of the content I plan to use I will check with my contact in the college.

User signature

I agree to follow this Acceptable Use Agreement and to support online safety throughout the college.

Signature ……………………………………………………………………………………… Date ……………………………………

Full Name ………
(printed)

Role……