The Chesterfield College Group

IT Acceptable Use Policy

Family:	Information Governance
Reference Code:	INF02
Manager Responsible:	Head of ICT
Committee for Approval:	Finance and Corporate Services
Approval Date:	June 2022
Issue Date:	July 2022
Review Date:	June 2025

Impact Assessment status	In preparing the Policy, any potential disproportionate impact it might have upon individuals with protected characteristics, as defined in the Equality Act 2010, have been carefully considered. It is the conclusion of the College Group that the Policy does not adversely impact on individuals with any of the protected characteristics.
Issue Number	5
Issue Date	July 2022
Review Date	June 2025
Originator	Head of ICT
Responsibility	Head of ICT

Contents

Aim

The policy aims to ensure that:

1. The Chesterfield College Group's IT facilities are used in furtherance of the organisation's mission and strategic priorities: safely, lawfully, and equitably.

2. All users of the Chesterfield College Group's IT facilities have a clear understanding of what constitutes acceptable and unacceptable use.

3. Access to the Chesterfield College Group's IT facilities is properly controlled and monitored to safeguard users and the organisation.

Scope

This policy and associated operating procedures apply to Chesterfield College, which includes Learning Unlimited, and to our subsidiary companies; Training Services 2000 Ltd (LU Derby), Learning Unlimited ATA Ltd, Recruit Unlimited Ltd and Chesterfield College Enterprises Ltd.

The policy and its associated procedures apply to all staff, students, apprentices (including remote students and apprentices), and other College users including governors, volunteers, external contractors, agency staff, and anyone working on the College premises or on behalf of the College.

The policy applies to anyone using the IT facilities provided or arranged by the Chesterfield College Group including, but not limited to, hardware, software, data, network access, third party services, online services, and IT credentials.

Implementation

The Chesterfield College Group will ensure that:

1. Meetings are held which introduce staff to the concept of an IT Acceptable Use Policy and to this policy and related procedures and guidelines (e.g., through staff induction, College Management Team, workforce development training) to enable ongoing dialogue around the acceptable use of the Chesterfield College Group's IT facilities.

2. Users of the Chesterfield College Group's IT facilities receive a level of training appropriate to their role, with refresher training annually. This is recorded and monitored through Workforce Development.

Communication Flow

The policy is approved by the College's Finance and Corporate Services Committee.

The policy is communicated to all staff through staff induction, the staff intranet, Virtual Learning Environment (VLE), email, training, and refresher training. It is communicated to students via induction and the VLE.

Awareness and acceptance of this policy is a probationary requirement for new staff.

The Simplified Code (Appendix 1) is communicated to users when logging onto a College computer. Acceptance is required to continue with logon.

Users of the College's IT facilities receive a level of training appropriate to their role, with refresher training annually. This is recorded and monitored through Workforce Development.

Monitoring

The implementation of the IT Acceptable Use Policy is continuously monitored by the Head of ICT and assured by the Vice Principal Finance and Corporate Services.

Associated Information and Guidance

There are many items of legislation that are particularly relevant to the use of IT, including:

- Computer Misuse Act 1990
- Copyright, Designs and Patents Act 1988
- Counter-Terrorism and Security Act 2015
- Criminal Justice and Immigration Act 2008
- Data Protection Act 2018
- Defamation Act 1996 and Defamation Act 2013
- Equality Act 2010
- Freedom of Information Act 2000
- Freedom of Information (Scotland) Act 2002
- Human Rights Act 1998
- Investigatory Powers (Interception by Businesses etc. for Monitoring and Record-keeping Purposes) Regulations 2018
- Keeping Children Safe in Education 2021 (statutory guidance)
- Obscene Publications Act 1959 and Obscene Publications Act 1964
- Police and Criminal Evidence Act 1984
- Police and Justice Act 2006
- Prevention of Terrorism Act 2005
- Privacy and Electronic Communications (EC Directive) Regulations 2003 (as amended)
- Protection of Children Act 1978
- Protection of Freedoms Act 2012
- Regulation of Investigatory Powers Act 2000
- Safeguarding Vulnerable Groups Act 2006 (Schedule 4 amended 2012)
- Terrorism Act 2006
- Working Together to Safeguard Children 2018 (statutory guidance)

Related Chesterfield College Group Policies and Documents

The related documents below can be found on the staff intranet:

- Data Protection Policy – INF03
- Staff Disciplinary Policy – PHR20
- Student/Apprentice Disciplinary Policy – TLA03
- Information Security Policy – INF01
- Safeguarding Policy – GOV05
- Staff Code of Conduct – PHR19
- Tackling Extremism & Radicalisation Policy – GOV06

Appendices

Documentation

- Appendix 1: Simplified Code
- Appendix 2: Core Regulations
- Appendix 3: Guidance Notes

Appendix 1: Simplified Code

The following is a summary of the main points of the IT regulations. You are expected to be familiar with the full regulations, which are available on the VLE and the staff intranet.

Governance

Do not break the law, do abide by the Chesterfield College Group's regulations and policies, and do observe the regulations of any third parties whose facilities you access.

Identity

Do not allow anyone else to use your IT credentials, do not disguise your online identity and do not attempt to obtain or use anyone else's.

Infrastructure

Do not put the College's IT facilities at risk by introducing malware, interfering with hardware, or loading unauthorised software.

Information

Safeguard personal data, respect other people's information and do not abuse copyright material. Remember that mobile devices may not be a secure way to handle information.

Behaviour

Do not waste IT resources, interfere with others' legitimate use, or behave towards others in a way that would not be acceptable in the physical world.

Appendix 2: Core Regulations

The issues covered by these regulations are complex and you are strongly urged to read the accompanying Guidance Notes, which give more detailed information (Appendix 3).

1. Scope

These regulations apply to anyone using the IT facilities (hardware, software, data, network access, third party services, online services, or IT credentials) provided or arranged by the Chesterfield College Group.

2. Governance

When using IT, you remain subject to the same laws and regulations as in the physical world.

It is expected that your conduct is lawful. Ignorance of the law is not considered to be an adequate defence for unlawful conduct.

When accessing services from another jurisdiction, you must abide by all relevant local laws, as well as those applicable to the location of the service.

You are bound by the Chesterfield College Group's general regulations when using the IT facilities.

You must abide by the regulations applicable to any other organisation whose services you access, such as Janet, Eduserv, and Jisc Collections.

When using services via eduroam you are subject to both the regulations of the Chesterfield College Group and the institution where you are accessing services.

Some software licences procured by the Chesterfield College Group will set out obligations for the user; these should be adhered to. If you use any software or resources covered by a Chest agreement, you are deemed to have accepted the Eduserv User Acknowledgement of Third-Party Rights. *See accompanying guidance for more detail.*

Breach of any applicable law or third-party regulation will be regarded as a breach of these IT regulations.

3. Authority

These regulations are issued under the authority of the College Corporation.

The Head of ICT is responsible for their interpretation and enforcement and may also delegate such authority to other people.

You must not use the IT facilities without the permission of the Head of ICT.

You must comply with any reasonable written or verbal instructions issued by people with delegated authority in support of these regulations. If you feel that any such instructions are unreasonable or are not in support of these regulations, you may appeal to the Head of ICT, the Vice Principal People and Culture, or via Chesterfield College Group's normal complaints handling procedures.

4. Intended Use

The IT facilities are provided for use in furtherance of the Chesterfield College Group's mission, for example, to support a course of study, research, or in connection with your employment by the College.

Use of these facilities for personal activities (provided that it does not infringe any of the regulations and does not interfere with others' valid use) is permitted, but this is a privilege that may be withdrawn at any point.

Use of these IT facilities for non-College commercial purposes, or for personal gain, requires the explicit approval of the Head of ICT, the Vice Principal People and Culture, and a senior post holder.

Use of certain licences is only permitted for academic use and where applicable to the code of conduct published by the Combined Higher Education Software Team (CHEST). See the accompanying guidance for further details: http://www.eduserv.ac.uk/services/Chest-Agreements.

5. Identity

You must take all reasonable precautions to safeguard any IT credentials (for example, a username and password, email address, smart card, soft token or other identity hardware or software) issued to you. You must not allow anyone else to use your IT credentials. Nobody has the authority to ask you for your password and you must not disclose it to anyone.

You must not attempt to obtain or use anyone else's credentials.

You must not impersonate someone else or otherwise disguise your identity when using the IT facilities.

You must comply with the Minimum Password Requirements detailed in the Information Security Procedures (INF01P).

6. Infrastructure

You must not do anything to jeopardise the integrity of the IT infrastructure by, for example, doing any of the following without approval:

- Damaging, reconfiguring, or moving equipment.
- Loading software on the Chesterfield College Group's equipment, other than with written authorisation from the Head of ICT.
- Reconfiguring or connecting equipment to the network other than by approved methods.
- Setting up servers or services on the network.
- Deliberately or recklessly introducing malware.
- Attempting to disrupt or circumvent IT security measures.

7. Information

If you handle personal, confidential, or sensitive information, you must take all reasonable steps to safeguard it and must observe the Chesterfield College Group's Data Protection Policy, Information Security Policy, and Mobile Device and Data Security Guidance, available on the staff intranet, particularly with regard to removable media, mobile and privately owned devices.

You must not infringe copyright or break the terms of licences for software or other material.

You must not attempt to access, delete, modify, or disclose information belonging to other people without their permission, or explicit approval from the Head of ICT or the Data Protection Officer.

You must not create, download, store or transmit unlawful material, or material that is indecent, offensive, threatening, or discriminatory. To protect yourself, others and the organisation, explicit written authorisation must be obtained prior to undertaking valid activities involving such material. The Head of ICT is the initial point of contact for such requests.

The Chesterfield College Group has guidelines and expertise to support the publication of information via the IT facilities in line with the College's mission, vision, and strategic priorities. You should contact the Marketing Team for guidance before using the IT facilities to publish information.

8. Behaviour

Real world standards of behaviour apply online and on social networking platforms, such as Facebook, Blogger and Twitter.

You must not cause needless offence, concern, or annoyance to others. For example: viewing or sending explicit images, engaging in online bullying, propagating racist, radical or extremist views or 'fake news'.

You should also adhere to Chesterfield College Group's guidelines on social media.

You must not send 'spam' (unsolicited bulk email) or unsolicited commercial email (UCE).

You must not deliberately or recklessly consume excessive IT resources such as processing power, bandwidth, or consumables.

You must not use the IT facilities in a way that interferes with others' valid use of them.

You must not use the IT facilities for any activity promoting terrorism or radicalisation or any activity covered by the Counter-Terrorism and Security Act 2015 or the Prevent Strategy 2011.

9. Monitoring

The Chesterfield College Group monitors and records the use of its IT facilities for the purposes of:

- The effective and efficient planning and operation of the IT facilities.
- Prevention, detection, and investigation of infringement of its regulations.
- Investigation of alleged misconduct.
- Safeguarding and duty of care.
- Detection of any material promoting terrorism or radicalisation, or any other activity covered by the Counter-Terrorism and Security Act 2015 or the Prevent Strategy 2011, in line with these publications and subsequent guidance.

The Chesterfield College Group will comply with lawful requests for information from government and law enforcement agencies.

You must not attempt to monitor the use of the IT facilities without explicit prior written authorisation from the Head of ICT.

10. Infringement

Infringing these regulations may result in sanctions under the College's disciplinary processes. Penalties may include withdrawal of services and/or fines. Offending material will be taken down.

Information about infringement may be passed to appropriate law enforcement agencies, and any other organisations whose regulations you have breached.

The Chesterfield College Group reserves the right to recover from you any costs incurred as a result of your infringement.

You must inform the Head of ICT if you become aware of any infringement of these regulations.

Appendix 3: Guidance Notes

This guidance expands on the principles set out in the core regulations. It gives many examples of specific situations and is intended to help you relate your everyday use of the IT facilities to the do's and don'ts in the core regulations.

Where a list of examples is given, these are just some of the most common instances, and the list is not intended to be exhaustive.

Where terms like "Authority", "Authorised", "Approved" or "Approval" appear, they refer to authority or approval originating from the person or body identified in section 3, or anyone with authority delegated to them by that person or body.

1. Scope

1.1 Users

These regulations apply to anyone using the Chesterfield College Group's IT facilities. This means more than students and staff. It could include, for example:

- Visitors to the Chesterfield College Group premises.
- People accessing the College's online services from off campus.
- External partners, contractors and agents based onsite and using the College network, or offsite and accessing the College's systems.
- Tenants of the College, using the College's computers, servers, or network.
- Visitors using the College's Wi-Fi.
- Students and staff from other institutions logging on using eduroam.

1.2 IT facilities

The term "IT facilities" includes:

- IT hardware that the Chesterfield College Group provides, such as PCs, laptops, tablets, smartphones, and printers.
- Software that the College provides, such as operating systems, office application software, web browsers etc. It also includes software that the College has arranged for you to have access to, for example, special deals for students on commercial application packages.
- Data that Chesterfield College Group provides or arranges access to. This might include online journals, data sets or citation databases.
- Access to the network provided or arranged by the College. This would cover, for example, wired network connections, on-campus Wi-Fi, connectivity to the Internet from Chesterfield College Group computers.
- Online services arranged by the College, such as Office 365, JSTOR, or any of the Jisc online resources.

- IT credentials, such as the use of your College login, or any other token (email address, smartcard, dongle) issued by Chesterfield College Group to identify yourself when using IT facilities. For example, you may be able to use drop-in facilities or Wi-Fi connectivity at other institutions using your usual username and password through the eduroam system. While doing so, you are subject to these regulations, as well as the regulations at the institution you are visiting.

2. Governance

It is helpful to remember that using IT has consequences in the physical world.

Your use of IT is governed by IT specific laws and regulations (such as those in the current Policy), but it is also subject to general laws and regulations such as the Chesterfield College Group's general policies.

2.1 Domestic law

Your behaviour is subject to the laws of the land, even those that are not apparently related to IT such as the laws on fraud, theft, and harassment.

Examples of relevant items of legislation are given in the Associated Information and Guidance section of this policy.

So, for example, it is illegal to:

- Create or transmit, or cause the transmission, of any offensive, obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material.
- Create or transmit material with the intent to cause annoyance, inconvenience, or needless anxiety.
- Create or transmit material with the intent to defraud.
- Create or transmit defamatory material.
- Create or transmit material such that this infringes the copyright of another person or organisation.
- Create or transmit unsolicited bulk or marketing material to users of networked facilities or services, save where that material is embedded within, or is otherwise part of, a service to which the user or their user organisation has chosen to subscribe.
- Deliberately (and without authorisation) access networked facilities or services.

2.2 Foreign law

If you are using services that are hosted in a different part of the world, you may also be subject to their laws. It can be difficult to know where any particular service is hosted from, and what the applicable laws are in that locality.

In general, if you apply common sense, obey domestic laws and the regulations of the service you are using, you are unlikely to go astray.

2.3 General institutional regulations

You should already be familiar with the Chesterfield College Group's general regulations and policies.

These are available on the staff intranet and the VLE.

2.4 Third party regulations

If you use the Chesterfield College Group's IT facilities to access third party service or resources, you are bound by the regulations associated with that service or resource (the association can be through something as simple as using your College username and password).

Very often, these regulations will be presented to you the first time you use the service, but in some cases the service is so pervasive that you will not even know that you are using it.

Examples of this include:

2.4.1 Using Janet, the IT network that connects all UK higher education and research institutions together and to the Internet.

When connecting to any site outside of the Chesterfield College Group, you will be using Janet and will be subject to the:

- Janet Acceptable Use Policy - https://community.ja.net/library/acceptable-use-policy
- Janet Security Policy - https://community.ja.net/library/janet-policies/security-policy
- Janet Connection Policy – https://community.jisc.ac.uk/library/network-and-technology-policies/janet-network-connection-policy

The requirements of these policies have been incorporated into these regulations, so if you abide by these regulations, you should not infringe the Janet policies.

2.4.2 Using Chest agreements

Eduserv is an organisation that has negotiated many deals for software and online resources on behalf of the UK higher education community, under the common banner of Chest agreements. These agreements have certain restrictions that may be summarised as: non-academic use is not permitted, copyright must be respected, privileges granted under Chest agreements must not be passed on to third parties, and users must accept the User Acknowledgement of Third Party Rights, available at: www.chest.ac.uk/user-obligations/.

There will be other instances where the Chesterfield College Group has provided you with a piece of software or a resource.

2.4.3 Licence agreements

Users shall only use software and other resources in compliance with all applicable licences, terms, and conditions. *For more information, contact the ICT Services Helpdesk.*

2.4.4 Using eduroam

When connecting to eduroam, whether at the 'home organisation' (Chesterfield College Group) or when visiting another of the thousands of eduroam member organisations worldwide, users are bound by the eduroam (UK) Policy - https://community.jisc.ac.uk/library/janet-services-documentation/eduroamuk-policy.

In particular, when using eduroam at a 'Visited organisation', users: “Must abide by restrictions applied by the home organisation and by Jisc [and] by the visited organisation ... Where Regulations differ, the more restrictive applies".

3. Authority

These regulations are issued under the authority of the College Corporation.

The Head of ICT is responsible for their interpretation and enforcement and may also delegate such authority to other people.

Authority to use the College's IT facilities is granted by a variety of means:

- The issue of a username and password or other IT credentials.
- The explicit granting of access rights to a specific system or resource.
- The provision of a facility in an obviously open access setting, such as an institutional website, a self-service kiosk in a public area, or an open Wi-Fi network on the campus.

If you have any doubt whether you have the authority to use an IT facility you should seek further advice from the ICT Services Helpdesk.

Attempting to use the IT facilities without the permission of the relevant authority is an offence under the Computer Misuse Act.

For the avoidance of doubt, the Head of ICT is authorised to take appropriate steps to protect the Chesterfield College Group's IT infrastructure and services and to support investigations including, but not limited to, disabling accounts, disconnecting, or recalling equipment, and examining systems, logs and data. If you feel that any such action taken is unreasonable or is not in support of these regulations, you may appeal to a senior post holder or via Chesterfield College Group's normal complaints handling procedures.

4. Intended Use

The College's IT facilities, and the Janet network, that connects institutions together and to the Internet, are funded by the tax paying public. They have a right to know that the facilities are being used for the purposes for which they are intended.

4.1 Use for purposes in furtherance of the Chesterfield College Group's mission

The IT facilities are provided for use in furtherance of the College's mission. Such use might be for learning, teaching, research, knowledge transfer, public outreach, the commercial activities of the College, or the administration necessary to support the above.

4.2 Personal use

You may currently use the IT facilities for personal use provided that it does not breach the regulations, and that it does not prevent or interfere with other people using the facilities for valid purposes (for example, using a PC to update your Facebook page when others are waiting to complete their assignments).

However, this is a concession and can be withdrawn at any time.

Employees using the IT facilities for non-work purposes during working hours are subject to the same management policies as for any other type of non-work activity.

4.3 Commercial use and personal gain

Use of IT facilities for non-College commercial purposes, or for personal gain, such as running a club or society, requires the explicit approval of the Head of ICT, the Vice Principal People and Culture and a senior post holder. The provider of the service may require a fee or a share of the income for this type of use. *For more information, contact the ICT Services Helpdesk.*

Even with such approval, the use of licences under the Chest agreements and several other agreements for anything other than teaching, studying or research, administration or management purposes is prohibited, and you must ensure that licences allowing commercial use are in place.

5. Identity

Many of the IT services provided or arranged by the College require you to identify yourself so that the service knows that you are entitled to use it.

This is commonly done by providing you with a username and password, but other forms of IT credentials may be used, such as an email address, a smart card, a soft token or some other form of security device or application.

5.1 Protect identity

You must take all reasonable precautions to safeguard any IT credentials issued to you.

You must change passwords when first issued and at regular intervals as instructed. Do not use obvious passwords, and do not record them where there is any likelihood of someone else finding them. Do not use the same password as you do for personal (i.e., non-College) accounts. Do not share passwords with anyone else, even IT staff, no matter how convenient and harmless it may seem.

If you think someone else has found out what your password is, change it immediately and report the matter to the ICT Services Helpdesk.

Do not use your username and password to log in to websites or services you do not recognise, and do not log in to websites that are not showing the padlock symbol.

Do not leave logged in computers unattended. Lock the computer or log out if leaving the room and log out properly when you are finished.

Do not allow anyone else to use your smartcard or other security hardware or software. Take care not to lose them, and if you do, report the matter to IT immediately.

5.2 Impersonation

Never use someone else's IT credentials or attempt to disguise or hide your real identity when using the College's IT facilities.

However, it is acceptable not to reveal your identity if the system or service clearly allows anonymous use (such as a public facing website).

5.3 Attempt to compromise others' identities

You must not attempt to usurp, borrow, corrupt, or destroy someone else's IT credentials.

6. Infrastructure

The IT infrastructure is all the underlying elements that make IT function. It includes servers, the network, computers, printers, operating systems, databases and a whole host of other hardware and software that must be set up correctly to ensure the reliable, efficient, and secure delivery of IT services.

You must not do anything to jeopardise the infrastructure.

6.1 Physical damage or risk of damage

Do not damage or do anything to risk physically damaging the infrastructure, such as being careless with food or drink at a computer or playing football in a drop-in facility.

6.2 Reconfiguration

Do not attempt to change the setup of the infrastructure without authorisation, such as changing the network point that a PC is plugged in to, connecting devices to the network (except for Wi-Fi or Ethernet networks specifically provided for this purpose) or altering the configuration of the College's computers. Unless you have been explicitly authorised, you must not add software to or remove software from College computers.

Do not move equipment without authority.

6.3 Network extension

You must not extend the wired or Wi-Fi network without authorisation. Such activities, which may involve the use of routers, repeaters, hubs, or Wi-Fi access points, can disrupt the network and are likely to be in breach of the Janet Security Policy.

6.4 Setting up servers

You must not set up any hardware or software that would provide a service to others over the network without permission. Examples would include games servers, file sharing services, IRC servers or websites.

6.5 Introducing malware

You must take all reasonable steps to avoid introducing malware to the infrastructure.

The term malware covers many things such as viruses, worms, and Trojans, but is basically any software used to disrupt computer operation or subvert security.

It is usually spread by visiting websites of a dubious nature, downloading files from untrusted sources, opening email attachments you are not expecting (including unexpected attachments that appear to come from people you know and trust), or inserting media that have been created on compromised computers.

If you avoid these types of behaviour, keep your computer's operating system and applications up to date, keep your antivirus software up to date and switched on, and run scans of your computer on a regular basis, you should avoid this problem. On devices that are fully managed by the Chesterfield College Group updates and antivirus are centrally configured.

6.6 Subverting security measures

The Chesterfield College Group has taken measures to safeguard the security of its IT infrastructure, including things such as antivirus software, firewalls, spam filters, etc.

You must not attempt to subvert or circumvent these measures in any way.

7. Information

7.1 Personal, sensitive, and confidential information

During their work or studies, staff, and students (particularly students carrying out research activities) may handle information that comes under the Data Protection Act 2018 or is sensitive or confidential in some other way e.g., strategic plans or internal financial data. For the rest of this section, these will be grouped together as Protected Information.

Safeguarding the security of Protected Information is a highly complex issue, with organisational, technical, and human aspects. The College has policies on Data Protection and Information Security, and if your role is likely to involve handling Protected Information, you must make yourself familiar with and abide by these policies.

The Data Protection Policy includes details of how the Chesterfield College Group ensures compliance with the Data Protection Act 2018 and who to contact with any queries.

7.1.1 Transmission of Protected Information

When sending Protected Information electronically, you must use a method with appropriate security. Email is not inherently secure. Appropriate security will depend on the nature and extent of the Protected Information and the intended recipient (for example a data sharing agreement or other contractual protection is generally required, since the Chesterfield College Group retains responsibility for safeguarding Protected Information even if it is held by a third party).

Before sending Protected Information electronically, please contact the ICT Services Helpdesk to discuss the requirement and for guidance on appropriate safeguards.

7.1.2 Removable media and mobile devices

Protected Information must not be stored on removable media (such as USB storage devices, removable hard drives, CDs, DVDs) or mobile devices (laptops, tablet, or smartphones) unless they are appropriately encrypted, and the key kept securely. *Please contact the ICT Services Helpdesk in advance for guidance on appropriate safeguards.*

If Protected Information is sent using removable media, you must use a secure, tracked service so that you know it has arrived safely. *Please contact the ICT Services Helpdesk in advance for guidance on appropriate safeguards.*

7.1.3 Remote working

If you access Protected Information from off campus, you must make sure you are using an approved connection method that ensures that the information cannot be intercepted between the device you are using and the source of the secure service.

You must also be careful to avoid working in public locations where your screen can be seen.

Advice on working remotely with Protected Information is available from the ICT Services Helpdesk.

7.1.4 Personal or public devices and Cloud services

Even if you are using approved connection methods, devices that are not fully managed by the Chesterfield College Group should not be used to store Protected Information.

Guidance on the use of personal devices to access College services is available in the Information Security Policy and Procedures and from the ICT Services Helpdesk.

Protected Information must not be stored in personal Cloud services, such as Dropbox.

7.2 Copyright information

Almost all published works are protected by copyright. If you are going to use material (images, text, music, software), it is your responsibility to ensure that you use it within copyright law. This is a complex area, and guidance is available from the Learning Resources department. The key point to remember is that the fact that you can see something on the web, download it or otherwise access it, does not mean that you can do what you want with it.

The Chesterfield College Group's IT facilities must not be used to store works in breach of copyright, for example, a copy of a commercial DVD or other video, in breach of the relevant terms or use or licence agreement, or software for which the College does not hold an appropriate licence.

7.3 Others' information

You must not attempt to access, delete, modify, or disclose information belonging to other people without their permission, unless it is obvious that they intend others to do this (e.g., accessing information on a public website), or you have explicit approval from the Head of ICT or the Vice Principal Finance and Corporate Services.

Where information has been produced in the course of employment by the Chesterfield College Group, and the person who created or manages it is unavailable, the responsible line manager may request that it be retrieved for work purposes by contacting the ICT Services Helpdesk. Agreed procedure will then be followed, obtaining authorisation from the Head of ICT, the Vice Principal People and Culture, and a senior post holder before such a request is acted on. In accessing the required information, care must be taken not to retrieve any private information in the account, nor to compromise the security of the account concerned.

Private information may only be accessed by someone other than the owner under specific circumstances governed by College and/or legal processes.

7.4 Inappropriate material

You must not create, download, store or transmit unlawful material, or material that is indecent, offensive, defamatory, threatening, or discriminatory.

To protect yourself, others and the organisation, explicit written authorisation must be obtained prior to undertaking valid activities involving such material. The Head of ICT is the initial point of contact for such requests.

There is also a limited exemption covering authorised IT staff involved in the preservation of evidence for the purposes of investigating breaches of the regulations or the law. To protect both IT staff and users, written authorisation must be obtained from the Head of ICT before this is done.

7.5 Publishing information

Publishing means the act of making information available to the public, this includes through websites, social networks, and news feeds. Whilst the Chesterfield College Group generally encourages publication, there are some general guidelines you should adhere to:

7.5.1 Representing the institution

You must not make statements that purport to represent the College without the approval of the Head of Brand and Communications.

7.5.2 Publishing for others

You must not publish information on behalf of third parties using the College's IT facilities without the approval of the Head of Brand and Communications.

8. Behaviour

The way you behave when using IT should be no different to how you would behave under other circumstances. Abusive, inconsiderate, or discriminatory behaviour is unacceptable. You should not make derogatory remarks about staff, students, competitors, or any other person.

8.1 Conduct online and on social media

The Chesterfield College Group's policies concerning staff and students also apply to the use of social media. These include human resource policies, codes of conduct, acceptable use of IT and disciplinary procedures.

8.2 Spam and UCE

You must not send unsolicited bulk emails or chain emails or unsolicited commercial emails (UCE), other than in specific circumstances and via appropriate systems. Note that the main Chesterfield College Group email system is not an appropriate system for sending bulk email (for example to a group of potential students) and must not be used for this purpose. *Further advice on this is available from the ICT Services Helpdesk.*

8.3 Denying others access

If you are using shared IT facilities for personal or social purposes, you should vacate them if they are needed by others with work to do. Similarly, do not occupy specialist facilities unnecessarily if someone else needs them.

8.4 Disturbing others

When using shared spaces, remember that others have a right work without undue disturbance. Keep noise down (turn phones to silent if you are in a silent study area), do not obstruct passageways and be sensitive to what others around you might find offensive.

8.5 Excessive consumption of bandwidth/resources

Use resources wisely. Do not consume excessive bandwidth by uploading or downloading more material (particularly video) than is necessary. Do not waste paper by printing more than is needed, or by printing single sided when double sided would suffice. Do not waste electricity by leaving equipment needlessly switched on.

9. Monitoring

9.1 Institutional monitoring

See Section 9 of the Core Regulations *(Appendix 2)*.

9.2 Unauthorised monitoring

You must not attempt to monitor the use of the IT facilities without explicit prior written authorisation from the Head of ICT.

This would include:

- Monitoring of network traffic.
- Network and/or device discovery.
- Wi-Fi traffic capture.
- Installation of key logging or screen grabbing software that may affect users other than yourself.
- Attempting to access system logs or servers or network equipment.

Where IT is itself the subject of study or research, special arrangements will have been made, and you should contact your course leader/research supervisor for more information.

Note that going beyond the bounds of agreed special arrangements constitutes a significant breach of trust and professional ethics and is likely to result in disciplinary action being taken against you, which may extend to legal action.

10. Infringement

10.1 Disciplinary process and sanctions

Breaches of these regulations will be handled by the Chesterfield College Group's disciplinary processes.

This could have a bearing on your future studies or employment with the College and beyond.

Sanctions may be imposed if the disciplinary process finds that you have indeed breached the regulations, for example, imposition of restrictions on your use of IT facilities, removal of services, withdrawal of offending material, fines, and recovery of any costs incurred by the Chesterfield College Group as a result of the breach.

10.2 Reporting to other authorities

If the College believes that unlawful activity has taken place, it will refer the matter to the police or other enforcement agency.

10.3 Reporting to other organisations

If the College believes that a breach of a third party's regulations has taken place, it may report the matter to that organisation.

10.4 Report infringements

If you become aware of an infringement of these regulations, you must report the matter to the relevant authorities: in the first instance the Head of ICT or the Vice Principal People and Culture.