Acceptable Use Policy

1. Introduction

1.1 The aim of this policy is to provide a broad and general framework so that all users of CCG computers, telephones and Internet services have an understanding of their permitted use. This policy will not cover every single set of circumstances, and therefore all users are reminded to adhere to the broader spirit of the policy.

2. Revision History

Version	Date	Author	Summary of changes
5		Benjamin Phillips	Add revision history Add reference to Janet acceptable use policy Add reference to telephone recordings Change references from 'CSU' to 'IT Services' Revise clean desktop clauses Revise cyber essentials clauses

3. Scope of this policy

3.1 This policy applies to anyone using Information Technology (IT) facilities provided by Chichester College Group ("the Group"). This includes our workforce, students, governors, contractors and visitors. Throughout the policy these individuals will be referred to as "users".

3.2 IT facilities are vital to the operation of the Group. This policy sets out the framework within which users may use IT facilities.

3.3 The phrase "IT facilities" encompasses, but is not limited to computers, software, peripheral devices, identities issued by the Group, online or cloud-based resources, email, telephones, internet access, including WiFi and data stored within computer systems.

3.4 The term "personal data" carries the definition provided within the Data Protection Act. In this context the Group is considered a data controller.

3.5 The Group will seek the explicit agreement of all users that they have read and understood this policy. One method of collecting this agreement is through the induction checklist or the declaration form at the end of this policy. Users will also receive regular reminders that use of Group IT facilities must be compliance with this policy.

3.6 This policy should be read in conjunction with:

- IT Security Policy
- Data Protection Policy
- Records Retention Policy
- Janet Acceptable Use Policy (https://community.jisc.ac.uk/library/acceptable-use-policy)

4. Distribution

4.1 This policy, along with all policies, are available on the staff intranet. All staff will be made aware of where to find Group policies, including this policy, during their induction.

4.2 A short-form version of this policy is displayed during the computer login process.

5. Acceptable use

5.1 In general:

- IT facilities are provided as resources to support the day-to-day business of the Group, for example in following a programme of study. If you are in doubt as to whether a planned use of these resources is business related, you should consult your line manager in the first instance.

- You must not intentionally interfere with the operation of IT facilities, Group computer, network or telephony systems; or connect or disconnect any devices; or install any software; to attempt to gain access to restricted systems without prior approval of IT Services.

- A user identity may only be used by the person who it is issued to. That individual is responsible for the use and protection of the credentials.

- Software must only be used in accordance with the terms of the license.

- Users will be required to use a unique password which meets the complexity requirements and is updated outlined within National Cyber Security Centre guidance, and the IT Security Policy.

- Users must either log off or lock their workstation when leaving their computer, tablet or mobile device unattended to prevent unauthorised access to the IT facilities.

- Users must maintain a 'clean screen' to ensure screens are not sited such that the information displayed on them can be easily seen by unauthorised people or captured by cameras or other recording devices in the vicinity. Users must also consider information open on the device to ensure personal and sensisitive information is not indivertibly shared when sharing the screen through video conferencing software.

- Users must maintain a 'clean desk', ensuring any paperwork and removable media is locked away before leaving the desk unattended.

- Users are required to comply with all legal, statutory and contractual obligations that are relevant to their role.

- On leaving the Group, users must inform their line manager prior to departure of any important information held within their account.

5.2 Data protection requirements are:

- All staff must comply with the Group Data Protection policy in their handling of personal data.

- The creation of student datasets outside of the Group Management Information System must first be approved by the Director of Information and Funding. You may be required to complete a Data Protection Impact Assessment before approval is granted.

- Users must not store personal data on mobile devices (tablets, smart phones, smart watches, tablets, etc.) or portable storage (USB keys, removable hard disks, etc.) or cloud storage services not provided by the Group (Dropbox, OneDrive, etc.) without a risk assessment having been approved by the Director of Information Technology. The risk assessment may take the form of a Data Privacy Impact Assessment.

- Users must take precautions to protect all computer media and mobile devices when carrying them outside the Group premises (e.g. avoid leaving a laptop unattended or on display in a car such that it would encourage an opportunist theft).

- Any exchange of classified data, including personal data, with external bodies must be done securely. Secure methods of exchanging data will include encryption, direct transfer and the use of trusted third parties. Such exchange of data must also be within the use permitted by the Group's data protection policy and notices, or permission will be sought from the individuals concerned.

- Sending personal data by fax is not permitted. Fax should be considered insecure and therefore not suitable for sending or receiving any information higher than the 'public' classification.

5.3 Privacy requirements are:

- Access to a member of staff's electronic mail and file storage may be given to the line manager or another member of staff as delegated by the line manager. Such requests must be placed in writing to the Director of Information Technology by the manager and access will only be given where there is a clear business case.

- User's electronic mail and file storage may be searched and access to information provided to comply with statutory requirements. This includes the Group's obligations under data protection and freedom of information

legislation.

- Since access to the file store and electronic mail may be given to others without a user's consent, users must not assume that their file store or electronic mail is private. Matters of a personal confidential nature must not be stored on or transmitted through Group IT facilities.

- The Group monitors the use of its computer and telephony systems to maintain efficiency and guard against misuse. Monitoring is also conducted to identify and escalate safeguarding concerns.

- The Group may monitor telephone calls for the purposes of ensuring satisfactory levels of customer service. If a call is to be monitored, notification will be given to all parties involved in the call.

- Incoming calls to the Group landlines are recorded until diverted to a new extension number by the switchboard. This processing is covered in a privacy notice on the Group website and in an automated message at the start of the call.

- Users are required to protect any classified information sent, received, stored or processed, by themselves according to the level of classification assigned to it, including both electronic and paper copies. Any materials the user creates must be appropriately labelled.

- Users must be aware of their working environment to ensure they are not overlooked or overheard by unauthorised people when working and must take appropriate care when working with classified information.

5.4 Electronic mail requirements are:

- A Group 'disclaimer' or 'footer' will be added to all outgoing electronic mail.

- All email conversations with external parties must be considered as being on Group headed stationery and appropriate standards of etiquette and formality adopted. Emails should be written using best practice email etiquette. The British Library guide is one example of best practice email etiquette.

- Users will ensure that they have entered the correct recipient email address(es) before sending the message, so that classified information is not compromised. Where the email address should not be disclosed, it must be

placed in the blind carbon copy field.

- Users must not represent their own views as those of the Chichester College Group or imply the formation of a contract between the Group and a third party.

- Material must not intentionally be sent, received or forwarded on, that may be considered as obscene, illegal or defamatory or which is intended to annoy, harass or intimidate another person.

- All electronic mail will be subject to automated scanning to identify viruses and unsolicited bulk mail (also known as 'spam'). Any email originating from blacklisted addresses will not be accepted.

- Electronic mailboxes will be capped in size and purged of aged items without notice. Retention schedules will apply to the Group electronic mail system. You should refer to the 'records retention policy' for the retention schedules which apply to each mailbox folder.

5.5 The Internet requirements are:

- The Group will log and filter internet usage by our users in accordance with our sector and statutory requirements.

- The unapproved use of instant messaging or peer-to-peer file sharing software is not permitted.

- Users must not upload or download materials in violation of copyright.

- Users must not access or distribute material which does not embody the core values of the group. This includes material which could be considered obscene, illegal, defamatory or which may harass or intimidate others.

5.6 Use of personal devices:

- Use of personally owned devices, to access Group systems, is at the risk of the owner and the Group accepts no liability.

- Holding Group related personal data on personally owned devices is discouraged and appropriate security measures must be put in place to ensure that the personal data is safeguarded from unauthorised disclosure. A device is deemed to have appropriate security measures if it meets all of the criteria in the current cyber essentials specification available on the ISAME

website.

- Enrolment of a personal device in a Group service where Group related personal data may be transferred to the device implies acceptance that the Group may:

  - Remotely wipe the data should the individual leave the Group's employment or the device is misplaced.

  - Enforce a minimum level of security remotely (e.g. encryption, PIN access, screen locking).

  - Require the installation of additional software on the device to support secure use of the service (such as Microsoft Authenticator to support multi-factor authentication).

5.7 The primary purpose of the provision of computer, network or telephony systems is in support of the business of the Group. Limited personal use is permitted within the terms of this policy and the following:

- Priority must always be given to the primary purpose of the service.

- Personal use must not interfere with the proper operation of the service.

- Personal use of the Internet is only made outside the working day (or during break times) and must not affect the performance of the user's duties.

- Personal use must not be in connection with the running of a business or in conflict with a staff member's responsibilities as an employee of the Group.

- The Group reserves the right to recover the costs of excessive personal use.

6. Consequences of misuse

6.1 Non-compliance with this policy may result in disciplinary action. Access to computer and telephony facilities may be withdrawn pending the outcome of an investigation or disciplinary action.

6.2 It is the Group's legal responsibility to refer downloading, viewing or storing of some materials (for instance illegal images of minors) to the Police.

6.3 If a user detects, suspects or witness an incident that may be a breach of security or if they observe any suspected information security weaknesses in systems or

services, they must report these immediately to the Data Protection Officer.

7. Status of this policy

7.1 This policy has been built using best practice from ISO27001 and forms part of the Group's commitment to achieving and maintaining cyber security certifications.

7.2 The operation of this policy will be kept under review by the Group Director of Information Technology.

Date reviewed: July 2023
Reviewed By: Group Leadership Team
Next review date: July 2025

Acceptable Use Policy Declaration

Any user of Group IT facilities who has not signed a contract of employment with the Group must read and accept the Acceptable Use Policy, sign the following statement and return this page to HR before any PC log-ins can be requested.

This signed declaration must be provided to IT Services with the PC log-ins request submitted to the CSU helpdesk.

Declaration

I confirm that I have read and understood the Acceptable Use Policy and that I must abide by it at all times.

I am aware that any breaches of this policy may result in the withdrawal of IT access and further action.

Name: _____

Signed: _____

Date: _____