IT Security Policy

1. Introduction

1.1 The confidentiality, integrity and availability of the Chichester College Group's (hereafter referred to as 'Group') Information Technology (IT) assets are vital to the operation of the Group and the success of its learners.

1.2 The degree of risk posed from a wide range of internal and external threats increases daily. The Group may be the target of attacks including those resulting in denial of vital services, vandalism and the theft or loss of personal data.

1.3 Legislation requires the Group to ensure that personal data is protected to the best of our abilities and only used in accordance with the purposes it was collected. Failure to do so runs the risk of substantial fines, breach of the trust that data subjects put in us and significant adverse publicity. Relevant legislation includes:

- Data Protection related legislation
- Computer Misuse Act
- Regulation of Investigatory Powers Act
- Telecommunications (Lawful Business Practices) Regulations

1.4 It is intended to follow best practice recommendations of bodies such as the British Standards Institute (BSI) wherever possible.

2. Scope

2.1 This Policy applies to all IT related systems and processes planned or in use by the Group or its sub-contractors.

If you intend to print a copy of this document, please check the issue number against the document held on the Group Intranet to ensure that only the current issue is used.

2.2 Other policies are linked to this policy:

- The Acceptable Use Policy
- The Document Retention Policy
- The Data Protection Policy
- The Bring Your Own Device Policy

3. Virus and malware protection

3.1 The Group maintains a current subscription to a mainstream Virus and Malware protection suite covering all asset types.

3.2 All Group assets including desktop PCs, laptops and servers must be protected by the standard Virus and Malware protection suite.

3.3 Incoming and outgoing email must be scanned for viruses and Malware by a suitable product. Any suspect messages are quarantined.

3.4 All web accesses must be virus and Malware scanned by the Unified Threat Management (UTM) services on the corporate firewall.

3.5 All removable media (USB storage, CDs, floppy disks) must be scanned before use.

4. Perimeter defence

4.1 The Group must maintain an appropriate, resilient, UTM device including firewalling, web content filtering, application filtering and virus and Malware scanning.

4.2 All access to/from Group resources to/from the Internet must be directed through this UTM device.

4.3 UTM policies must be created based on allowing the least access necessary for the application.

4.4 UTM policies must limit workstations to HTTP/HTTPS access to the Internet unless there is a valid business reason to do otherwise.

5. Internal network

5.1 Definitions

5.1.1 A ‘foreign’ device is any device that is not owned and maintained by the Group’s Computer Service Unit.

5.1.2 Physical connection is connection of a device directly to the network via a cable.

5.1.3 A ‘network lab’ is a specialist area of the network where students and staff are permitted to attach equipment and reconfigure infrastructure components for curriculum related purposes.

5.2 Physical connection of ‘foreign’ devices can cause significant disruption to the operation of the network resulting in loss of access to services.

5.2.1 Physical connection of any ‘foreign’ device to the Group network infrastructure is prohibited unless explicitly agreed by Computer Services.

5.3 Connection of any device to the Group network carries an implicit right of access to that device by the Group. This access right may be utilised where a device is suspected to be the cause of security or operational problems or during the investigation of abuse.

5.4 Network access may be disabled without notice in any area of the Group network, or connected device, suspected to be a threat to the integrity of the network.

5.5 Network labs must be physically separate networks; no infrastructure is shared and no access permitted to the main Group network.

6. Wireless networking

6.1 Wireless networking is the primary route via which 'foreign' devices are given access to the Internet and Group systems.

6.2 The Wireless network is firewalled away from the main Group network.

6.3 The Wireless network is secured according to the best practice at the time and reviewed regularly.

6.4 Any Group owned asset requiring access to internal Group resources must do so via a Virtual Private Network (VPN).

6.5 Access is only provided to authenticated users.

7. Physical security

7.1 Key infrastructure locations are defined as server rooms, core network cabling closets or any location vital to the operation of Group systems.

7.2 Key infrastructure locations are protected by an independent alarm zone not set or unset as part of locking/unlocking the building.

7.3 Access to Key infrastructure locations is be restricted to Computer Services Unit staff or others explicitly approved by the IT Director.

7.4 Key infrastructure locations are additionally secured via code lock.

7.5 Contractors working in key infrastructure locations are supervised at all times.

7.6 Key infrastructure locations containing servers or significant concentrations of active networking equipment must have redundant cooling systems sufficient to maintain equipment within manufacturers recommended operational temperatures. Over temperature alarms notifying key staff of over temperature alerts are installed.

7.7 Key infrastructure locations must be protected by uninterruptable power supplies capable of sustaining the equipment for an appropriate period.

7.8 Where IT assets are installed in vulnerable positions suitable security equipment must be used to prevent theft. For instance a projector installed in a relatively insecure portacabin needs additional security such as a secure mount and cable.

8. Patch and vulnerability management

8.1 Patch management

8.1.1 All operating systems and software components are patched to the manufacturer's current recommendations. Where patching is not possible then the insecure systems risk process is invoked.

8.2 Vulnerability management

8.2.1 Systems are regularly scanned for vulnerabilities and mitigations put in place for non-critical issues. Where significant vulnerabilities are discovered the insecure systems risk process is invoked.

8.2.2 The Group will engage an external contractor to conduct a yearly perimeter penetration test. Issues detected during the penetration test will be addressed using the insecure systems risk process.

8.3 Insecure systems risk process (ISRP)

8.3.1 The purpose of this section is to identify and protect Group assets that are of particularly high risk. Either because they contain highly critical, or sensitive information such as financial or personal, or because they are inherently difficult to protect.

8.3.2 The ISRP considers:

- *Likelihood.* For example, whether a system is exposed to an insecure network or whether a remote compromise is possible.
- *Impact.* The impact of the system being compromised for example bad publicity, loss of business function or exposure of personal data.
- *Mitigation.* Whether mitigations can be put into place for instance the isolation of the system, upgrading to a new version or rewriting code.

This will be scored against a standard Group risk matrix which maps likelihood against impact. See appendix A for an example of the matrix.

8.3.3 Any system which scores within the “Extreme risk, immediate action” category must receive immediate attention such as disconnection from the Internet or closing down the system if immediate mitigations are not possible.

8.3.4 Any system that contains personal data or data related to the processing of credit card transactions (in terms of PCI-DSS) must be considered a 'Major' risk.

8.3.5 The output from the ISRP will be an action-plan with dates and responsibilities for mitigating the risk.

8.3.6 Consideration must be made of whether any insecure system must be added to the overall risk register.

9. Authentication

9.1 All users of Group systems are required to authenticate to systems before use.

9.2 The standard form of authentication is via username and password.

9.3 The Group will move towards a single set of authentication credentials across all systems to ease the use of systems.

9.4 Minimum standards for passwords are enforced:

- Passwords must be changed every 90 days
- Passwords are a minimum of eight characters in length
- Complexity requirements are applied. These requirements are, at a minimum, a mix of upper and lower case, a number and a symbol.
- Accounts will be locked-out after 10 invalid attempts during a 30-minute period after which it will be locked for 24 hours, requiring a call to the Help Desk to reset.

9.4.1 Never use your Group password for personal accounts.

9.4.2 Authentication information must not be shared with anyone else under any circumstances. It is a known malicious practice for individuals to pretend to be the service desk and to try to convince users to share their password. The legitimate service desk will ***never*** do this.

9.4.3 Some accounts are excluded from lockout and/or password change requirements for operational reasons although complexity requirements will still apply.

9.4.4 Multi-factor authentication will be used where there is an increased risk to personal data for instance where personal data can be accessed remotely or from mobile devices.

9.5 Privileged accounts

9.5.1 A privileged account is defined as an account that provides significantly higher levels of privilege than a normal user. Typically, these accounts are used to make significant configuration changes and have extended access to data.

9.5.2 A secure credential repository is maintained to hold privileged account details. Access to the credential repository is tiered according to need.

9.5.3 Privileged account passwords are changed on a regular basis and adhere to length and complexity requirements.

9.5.4 If a member of the systems team leaves then critical privileged account passwords are changed immediately.

9.6 User passwords are only changed by help desk staff when the identity of the person can be verified. Appropriate methods of verification include:

- Group photo ID card
- Other form of official photographic ID (passport, driving license)
- By verification of personal details (e.g. address, DOB)

10. Backup and recovery

10.1 Automated daily backups are taken of relevant Group systems.

10.2 Backups are 'proved' using test or operational restores on a regular basis.

10.3 Status of backups is checked and recorded daily. Records are retained for audit purposes.

10.4 At a suitable point backup tapes are moved to a secure off site location.

11. Electronic mail

11.1 Electronic mail is an insecure method of communication.

11.2 Under no circumstances must emails containing personal data be sent outside of the Group in plain text.

11.3 Personal use of the Group staff email system is not permitted.

11.4 Other members of staff may request access to an individual's email when they are absent. In this eventuality a request must be made in writing to the IT Director stating the reasons access is required and why it cannot be resolved via other means.

11.5 Wherever possible role-based email accounts must be used (e.g. accounts@chichester.ac.uk)

11.6 All email is scanned for viruses, Malware and to check whether it is unsolicited commercial email (UCE, aka SPAM). Messages detected as UCE or to contain viruses or Malware is deleted immediately. Suspect emails are quarantined.

If you intend to print a copy of this document, please check the issue number against the document held on the Group Intranet to ensure that only the current issue is used.

11.7 All email file attachments that may be of file types known to harbour Malware or viruses are quarantined.

11.8 Outgoing mail is rate limited to prevent a compromised email account being used to send UCE from the Group email domain. This may be bypassed on request for particular business needs.

11.9 Individuals must take care to ensure that the phrasing of electronic messages do not accidentally imply the formation of a contract between the Group and another person or company. Electronic mail carries the same validity as a letter.

11.10 Users of the Group email system are encouraged to regularly purge their email accounts of older emails.

11.11 Particular care should be taken when sending either emails to groups of individuals, inside or external to the Group. It is a breach of this policy as well as the Data Protection Policy (and a breach of Data Protection legislation) to send such emails so that recipients can see the details of other recipients. In ALL circumstances, such emails should use the bcc option.

12. Encryption

12.1 In general, the holding or transfer of personal or sensitive data on email, file transfer services, removable media or on laptops is strongly discouraged. If unavoidable, the use of encryption is mandatory.

12.2 Advice on the use and relevance of encryption should be sought from Computer Services or from the data protection team.

13. File storage

13.1 Computer Services regularly issues best practice guidance as to where to securely store files. Approved cloud storage for Group data include Group maintained OneDrive, Sharepoint, Groups and Teams sites.

13.2 Student file storage.

13.2.1 The Group provides a student network drive for the temporary ‘working’ storage of student files. Students are responsible for keeping independent backups of their own work and the Group accepts no responsibility for its safekeeping.

13.2.2 Disk space quotas are enforced for student network drives. Extension of quotas only takes place after an assessment of need.

13.2.3 Lecturers are given access to student accounts on request but only in support of teaching and learning.

13.2.4 Student accounts that have been inactive for 9 months are deleted. No copies are retained. This is to allow efficient management of student file storage resources.

13.2.5 Additional file storage for students is made available via Microsoft OneDrive. The Group takes no responsibility for the safekeeping of files stored on this service, which is operated by Microsoft.

13.3 Staff file storage.

13.3.1 The Group provides file storage areas for members of staff, which may be limited in size and is for the storage of business related files only.

If you intend to print a copy of this document, please check the issue number against the document held on the Group Intranet to ensure that only the current issue is used.

13.3.2 A line manager may request access to an individual's file storage when they are absent. In this eventuality, a request must be made in writing to the IT Director stating the reasons access is required and why it cannot be achieved via other means.

13.3.3 Staff accounts are deleted after one year of inactivity. This is to allow efficient management of staff file storage resources.

14. **Use of mobile devices**

14.1 Personal devices

14.1.1 A personal device is any device that is owned by the individual and not the Group. This includes laptops, home computers, smart phones and tablets.

14.1.2 Owners of personal devices choosing to access Group systems do so at their own risk.

14.1.3 Personal data must not be held on personally owned devices unless appropriate security measures are put in place to ensure that the personal data is adequately safeguarded in compliance with the requirements of Data Protection legislation, the Group Data Protection Policy and this policy.

14.1.4 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 Group data from the device.
- Enforce a minimum level of security remotely (e.g. encryption, PIN access, screen locking) by assuming control of security settings on the device.
- Install additional software on the device to support secure use of the service.

14.1.5 Use of Group software is only permitted in compliance with the software license held by the Group. In practice this usually means that Group software may not be installed on personal devices.

14.2 Group owned mobile devices

14.2.1 All Group owned mobile devices are subject to regular recall for the purposes of applying updates and an inventory check.

14.2.2 Group owned mobile devices may require regular connection to the Internet to ensure that updates are applied. Failure to apply updates may result in the device being locked and requiring return to the Computer Services Unit.

14.2.3 If personal data is stored on a Group owned mobile device then the device must be encrypted and password protected to industry standards.

15. Contracts & procurement

15.1 In any procurement of a device or system there must be a formal appraisal of security and data protection considerations, including compliance with the Group Data Protection Policy.

15.2 In any contracts related to IT systems there must be a clause that requires the vendor to promptly address any security issue with the system. This obligation will be binding for the life of the system whilst it is under a support contract. Failure in this respect will be considered breach of contract.

16. Use of online (‘cloud’) file storage services by staff

16.1 The only supported online file storage services are Group maintained Microsoft OneDrive, Sharepoint, Groups and Teams sites which are accessed via Group authentication services and where data is held in accord with JISC negotiated

Data Protection amendments to the Office 365 end user license agreement.

16.2 Other online file storage services must not be used for the storage of personal data since the data is commonly stored outside the EEA which does not comply with the Principles of the Data Protection legislation and the Group Data Protection Policy.

16.3 The use of data synchronisation tools where secure data is replicated to the cloud (for instance OneDrive Synchronisation Tool) will not be permitted since data can easily be replicated to insecure assets.

17. Disposal of IT assets

17.1 Data remnants: All Group devices or components capable of storing data must be securely erased as part of the disposal process. In the case of PCs this is a responsibility of a third-party disposal agent who provides documentary evidence of secure erasure.

17.2 Any disposal of electronic equipment must follow the waste electrical and electronic equipment (WEEE) directive.

18. Logging, monitoring and filtering

18.1 Logging and filtering must meet the requirements of the DoE statutory guidance “Keeping Children Safe in Education” for appropriate filtering and monitoring.

18.2 The use and operation of the IT infrastructure will be logged in order to ensure the efficient running of systems, allow the investigation of allegations of abuse and in support of legal obligations.

18.3 Access to raw log data will not be given. Expert interpretation of log files is necessary to ensure fairness in the investigative process.

18.4 Any requests for interpretation of log files must be made in writing to the IT Director and be in relation to an on-going disciplinary process.

19. Software development

19.1 Systems development must adhere to industry best practices in relation to security, data protection, development methodology, documentation and change management to ensure against the accidental exposure of personal or confidential data.

20. Status

20.1 This policy was approved by the Group leadership Team. It supersedes all previous documentation.

20.2 The operation of this policy will be kept under review by the IT Director. It may be reviewed and varied from time to time by the Group Leadership Team.

Date approved:	September 2018
Approved by:	Group Leadership Team
Date reviewed:	September 2018
Next review date:	July 2019

If you intend to print a copy of this document, please check the issue number against the document held on the Group Intranet to ensure that only the current issue is used.