Croydon College

COULSDON SIXTH FORM COLLEGE

Croydon University Centre

INFORMATION SECURITY POLICY
Approved by: Executive Committee
Date approved: 22 February 2022
Strategy/Policy Responsibility: Vice Principal Education & Quality
Review date: January 2024

Information Security Policy

1. PURPOSE

1.1 This policy defines a framework by which Croydon and Coulsdon College's Information Technology (IT) systems, data, assets, infrastructure and computing environment will be protected from threats whether internal, external, deliberate or accidental.

1.2 Information Systems are of primary importance in supporting College business and academic activities. The availability, security, confidentiality and data integrity of information systems is critical to the success of the College.

1.3 The term 'Employee' is used to describe all of those authorised to use College IT systems and equipment to carry out College business. This Policy covers all employees who work at Croydon and Coulsdon College including, but not limited to, Governors, managers, academic staff, business support staff, agency workers, consultants, trainees, students or apprentices on work placement in the College, as well as those on honorary contracts.

2. SCOPE

2.1 All College IT Systems, environments and the information contained within them will be protected against unauthorised access.

2.2 All use of the College's IT facilities must comply with the College's Information Technology (IT) and Monitoring Policy.

2.3 Information kept within IT systems will be managed securely, comply with the College's Information Policy, relevant data protection laws and satisfy the College's expectations that such assets will be managed in a robust and professional manner.

2.4 Directors, Heads of Schools and line managers have a responsibility for ensuring the implementation of, adherence to and compliance with this policy throughout their areas of functional responsibility.

2.5 The integrity and security of all IT systems and any information contained within these systems is the responsibility of IT Services.

2.6 All regulatory and legislative requirements regarding IT security and IT based information, confidentiality and integrity will be addressed by IT Services, MIS and the College.

2.7 All users have a responsibility to report promptly to IT Services any incidents which may have an IT security implication for the College.

2.8 All employees are required to familiarise themselves with this policy, to adhere to it and comply with its requirements. Any failure to comply with the policy may result in disciplinary action or other equivalent action.

3. THE IT ENVIRONMENT

3.1 The College’s IT Services department manage a range of central computing services including servers, core network switches, edge network switches, wireless (Wi-Fi) systems, IP and mobile telephony systems, CCTV systems, backup systems, Operating Systems, application software and the structured network cabling infrastructure servicing these systems and connecting the sites.

3.2 The IT environment is defined as all central computing resources and network infrastructure managed and overseen by IT Services and all computing devices that can physically connect to it, and have been authorised to connect to this environment. All are covered by this policy, including computing hardware and software, any College related data residing on these machines or accessible from these machines within the College network environment and any media such as portable storage or USB devices, CD, DVD, and backup tapes.

3.3 All temporary and permanent connections to the College network, the Wi-Fi network, Remote Desktop Infrastructure and any Virtual Private Networks (VPN) are similarly subject to the conditions of this policy.

3.4 IT equipment not owned by the College may be connected to the College’s network. However, all such equipment must comply with College guidance governing the use of IT resources.

3.5 IT Services reserves the right to monitor, log, collect and analyse the content of all transmissions on College networks at any time deemed necessary for monitoring performance, fault diagnostics and compliance with the Information Technology (IT) and Monitoring Policy and legal requirements.

4. PHYSICAL SECURITY

4.1 IT Services manage secure Server Room facilities with protected UPS power supplies and climate-controlled environments. Access to the Server Rooms are limited, monitored, and audited.

4.2 IT Services also support distributed Communications Rooms containing network equipment and cabling on each floor of both campuses. All of these distributed communication rooms are secure and checked regularly.

4.3 Any IT equipment in general office environments must be secured behind locked doors and protected by user log-out and/or password protected whenever it is left unattended and outside of general office hours.

4.4 Desktop PCs in public areas should contain a device or mechanism for securing and protecting the main components and contents of the PC from theft.

4.5 Any portable IT equipment such as laptops, tablets, smart phones, portable hard drives etc. should use a log-on or power-on password wherever available. Any unattended portable IT equipment should be physically secure, for example locked in an office or a desk drawer. When being transported in a vehicle they must be hidden from view.

5. AUTHENTICATION AND PASSWORD POLICY

5.1 To ensure the security and integrity of College data, the College requires the digital authentication of all users of the College systems, networks and printing devices. Identified and authorised users will securely authenticate to College systems and access only the resources that they have been authorised to access.

5.2 Authentication credentials will not be coded into systems, programs or queries unless they are encrypted, and only when no other reasonable option exists.

5.3 College IT and Management Information Systems (MIS) access is only available via authorised individual user accounts. These accounts are available to approved individuals only and authorised via the HR New User IT Access Request procedure available from HR.

5.4 Username and Passwords are used at the College for users to facilitate access to IT Resources. Poorly chosen passwords may result in the compromise of the College network and data.

5.4.1 Users should avoid passwords that are considered weak that include:

- Names of family, pets, friends or co-workers
- Birthdays or other personal information such as address
- Words or numbers patterns such as qwerty, abcde, 67890
- Any of the above spelled backwards
- Any of the above preceded or followed by a number eg. alan1, 1alan

5.5 Passwords must never be shared or revealed to anyone, including IT Services staff, beyond the authorised user. To do so exposes the authorised user to actions that the other party may take.

5.6 Passwords must never be written down and left in a place where unauthorised persons may discover them.

5.7 If an account or password is suspected to have been compromised, the password must be changed immediately and IT Services informed.

5.8 All vendor supplied default passwords such as default passwords supplied with routers, switches or software must be changed before initial use within the IT Environment.

5.9 Passwords must always be encrypted when held in storage or when transmitted over communication systems.

5.10 Password Policy

5.10.1 IT Services will ensure all network passwords follow at least Microsoft best practice recommendations

5.10.2 A valid password must consist of at least 8 characters.

5.10.3 The password must be a complex password containing three of the following categories:

- one uppercase letter
- one lower case letter
- one number (0-9)
- one non-alphanumeric character symbol (eg. # @ £)

5.10.4 Passwords’ maximum age is 60 days and users are prompted to change this

5.10.5 Passwords must be changed on first use of new accounts

5.10.6 Password history maintains a record of the last 6 passwords

5.10.7 PCs will be password locked after 10 minutes of inactivity

5.10.8 User accounts will be locked after 5 consecutive failed logon attempts

5.10.9 User accounts will then be locked out for a period of 30 minutes

6. DATA SECURITY

6.1 The College attaches great import to the secure management of the data it holds and generates and will hold employees accountable for any inappropriate mismanagement or loss of it.

6.2 To ensure that the College systems remain secure, Staff and Student networks are logically separated by the use of Virtual LAN technology (VLANS). The Network switches are configured to ensure that students cannot browse or access College business systems.

6.3 The College holds a variety of sensitive data including personal information about students and staff. All staff who have been given access to personal information must comply with their responsibilities under the College's Information Policy and Data Protection Law. For further guidance please refer to the College's Information Policy.

6.4 The College provides secure and practical remote access to information and data held within its various IT systems and IT infrastructure. In most cases, gaining access to such data via remote access will prove sufficient and safe for most needs and is the recommended general mode of remote use of such data and information. Remote access to college systems must be secured with additional Multi Factor Authentication (MFA).

6.5 Any copying, or original creation, of sensitive data and information onto any form of portable media device (USB device, CD, DVD, External Hard Drive, portable music player, Laptop, Tablet etc.) or Cloud Storage (Dropbox, Microsoft OneDrive, Google Drive, Apple iCloud etc.) or its transportation beyond the secure environment it was intended to be used within (systems environment, PC environment, office etc.) carries additional responsibilities for the individual undertaking such activity.

All reasonable alternatives should be considered and responsibilities should be clarified by performing a risk analysis, which considers the following rules/principles:

6.5.1 Employee or Student (personal) data should not leave the campus. In this context "leave" implies its physical transport to an external and insecure location. Remote access to such data through an individual's approved access levels and permissions is distinct and not intended to be included in the term "leave".

6.5.2 If it is a unique or master version of data/information that has not been safely copied to a secure electronic or physical location within the College's IT Environment (implying that its subsequent loss is irrecoverable) then a copy should be made and stored securely prior to its off-site transportation for use.

6.5.3 If, following such a risk analysis, an individual, in consultation with their line manager, identifies a business imperative to take sensitive data off campus they are not to do so without prior consultation with the College Data Protection Officer (DPO). Failure to comply with this requirement may be considered a serious breach of this policy.

7. STORAGE AND DISPOSAL OF CONFIDENTIAL INFORMATION

7.1 Confidential information must be stored in such a way as to ensure that only authorised persons can access it. The information should be kept secure, using, where practicable, dedicated storage such as network file servers rather than local PC hard disks, and an appropriate level of physical security. File or disk encryption should be considered as an additional layer of defence, where physical security is considered insufficient.

7.2 To ensure that compliance can be monitored and reviewed, logon access records will be logged, monitored and records kept for a minimum of six months, or for longer, where considered appropriate.

7.3 Identifying confidential information is a matter for assessment in each individual case, however, information will be considered confidential if it is of limited public availability; is confidential in its very nature; has been provided on the understanding that it is confidential; and/or its loss or unauthorised disclosure could have one or more of the following consequences:

7.3.1 Financial loss
e.g. the withdrawal of funding, a fine by the ICO or a legal claim for breach of confidence.

7.3.2 Reputational damage
e.g. adverse publicity, demonstrations, complaints about breaches of privacy.

7.3.3 An adverse effect on the safety or well-being of members of the College or those associated with it.
e.g. increased threats to staff or students engaged in handling sensitive data, embarrassment or damage to suppliers, staff and students.

7.4 Employees who store sensitive or confidential information on privately owned portable equipment must ensure that such data is thoroughly and securely erased from that equipment when they leave the College's employment. Employees should consult IT Services for assistance and guidance on appropriate clearing techniques and tools.

7.5 College printing and photocopying systems ensure that staff must first authenticate themselves to prevent unauthorised access to information. This ensures that confidential information can be printed and collected securely from the most convenient network device. Staff must ensure that all copies are removed and secured from printing devices once complete.

8. ENCRYPTION CONTROLS

8.1 Where the transport of personal, sensitive or confidential data from College systems is unavoidable, Employees must consult the College's Data Protection Officer (DPO) or IT Services to ensure that this data is fully encrypted to guarantee that the data is appropriately protected from unauthorised access.

8.2 In the case of personal data, the ICO recommends that all portable devices and media should be encrypted where the loss of the data could cause damage or distress to individuals.

8.3 IT Services will maintain a supply of 256-bit full AES Encrypted USB Flash Drives for the purpose of transporting personal, sensitive or confidential data.

8.4 The passphrase of any encrypted device must not be stored with the device.

9. LOSS OR THEFT OF CONFIDENTIAL INFORMATION

9.1 A data or IT security incident relating to breaches of security and/or confidentiality could range from IT users sharing passwords to the loss or theft of confidential or personal information either inside or outside the College.

9.2 A security incident is any event that has resulted or could result in:

9.2.1 The disclosure of confidential information to any unauthorised person

9.2.2 The disclosure of confidential information or passwords via any unauthorised website (Phishing)

9.2.2 The integrity of the system or data being put at risk

9.2.3 The availability of the system or information being put at risk

9.3 All incidents must be reported to your immediate line manager or to IT Services or in the case of a possible data breach to the Data Protection Officer (DPO) so that they may be investigated. Serious incidents should be reported immediately to the Director of IT & Estates. A written report should be submitted containing the following information:

- Date of discovery of the incident
- Who discovered the incident
- Details of the incident
- Location of the incident
- Action already taken if there is an immediate risk to the College
- Any action taken by the person discovering the incident at the time of discovery, eg report to police.

9.4 In the case of a serious potential breach, the Vice Principal Finance and Resources will initiate an investigation into the incident and will decide whether it needs to be reported to any regulatory bodies or other third parties, eg insurers, ICO etc. The Vice Principal Finance and Resources will retain a central register of all such incidents occurring within the College and provide a report to the Executive team.

9.5 In the case of a personal data breach, the Personal Data Breach Policy and Procedure will be followed. An investigation will be initiated by the Data Protection Officer (DPO) and a decision made as to whether it needs to be reported to any regulatory bodies or other third parties, eg insurers, ICO etc. All reports to the ICO will be shared with the Executive team.

9.6 The following is a list of examples of breaches of security and breaches of confidentiality. It is neither exclusive or exhaustive and should be used as a guide only. If there is any doubt as to what constitutes an incident, it is better to inform IT Services who will then decide whether a report should be made.

9.6.1 Examples of breach of security:

- Loss of portable media devices, eg non-full AES Encrypted USB memory sticks etc.
- Victim of a Phishing incident whereby you have given your college password out in response to an email / telephone call
- Loss of computer equipment due to crime or accident
- Accessing any part of a database using someone else's password
- Finding doors and/or windows broken and/or forced entry gained to a secure room/building in which IT equipment exists.

9.6.2 Examples of a breach of confidentiality:

- Finding confidential/personal information either in hard copy or on a portable media device outside College premises or in any of the College's public or common areas
- Finding any records about an employee, student, or applicant in any location outside the College's premises
- Passing information to unauthorised people either verbally, written or electronically.

10. SYSTEM LOGS AND EVENT LOGGING

10.1 The College will ensure that all security event logs, operational audit logs and error logs are properly reviewed and managed by qualified IT Services staff. The College will also ensure that other events such as the synchronisation of all computer system and CCTV clocks across all platforms will be regularly monitored.

10.2 The College will ensure that any unauthorised attempt to access or attack the College Infrastructure such as Denial of Service (DoS) attacks will be logged and automatic alerts sent to the Network team.

10.3 Anti-Virus infections will be recorded, logged and alerts automatically sent to the Network and Helpdesk team to ensure immediate quarantine and investigation.

10.4 All Backups will be logged and any backup failures will be automatically alerted to Network staff.

11. Specific Systems

11.1 File Storage

11.1.1 All Network Users have access to centrally managed file storage. Use of the file storage is controlled by central and authenticated access to IT Systems.

11.1.2 The College supports central storage of systems and data on College Servers and central Storage Area Networks (SANs) utilising, where possible, Server Virtualisation technology to reduce the number of physical servers it needs to support and procure.

11.1.3 For the vast majority of applications the security of files stored centrally is appropriate. In particular this means they will be backed up. However, if files require a higher level of security, staff can contact IT Services for assistance.

11.2 Email

11.2.1 Email is not a secure communication medium. All users should be conscious of this and consider how Emails might be used by others. Emails can easily be taken out of context and once an Email is sent you cannot control what the recipients might do with it. It is also very easy to forward large amounts of information or data.

11.2.2 Similarly users should not necessarily trust what they receive in an Email. In particular, users must be made aware of Phishing Emails and never respond to a request to provide personal data, usernames or passwords. Please see the Information Technology (IT) and Monitoring Policy for more information on Phishing.

11.2.3 Email should only be used to send personal or confidential data where the recipient is trusted, the information owner has given their permission, and appropriate security safeguards have been taken e.g. encryption.

11.3 The Internet

11.3.1 The College uses JANET (Joint Academic Network) provided by JISC for all its connections to the Internet and as such, all users of the College network are subject to the JANET Acceptable Use Policy.

https://community.ja.net/library/acceptable-use-policy

11.3.2 All College Network Users are provided with Internet Access via the HR New User IT Access Request procedure and are subject to acceptable use and as laid out in the College's Information Technology (IT) and Monitoring Policy.

11.3.3 The College secures its internet connections via firewall devices and Internet and Email filtering appliances.

11.3.4 All College Internet access is filtered, logged and monitored.

11.3.5 Users can access the Internet through an authenticated connection or via a secure Wi-Fi connection.

11.4 Remote Access to Systems

11.4.1 Any remote access must be controlled by secure access control protocols using appropriate levels of encryption and Multi Factor authentication.

11.4.2 Remote access to College systems is available only via the College's secure Remote Desktop Services connection.

11.4.3 Remote connections to any College IT systems or services are subject to the same rules and regulations, policies and practices just as if they were physically on the campus.

11.4.4 No other remote access service or Virtual Private Network (VPN) shall be installed or set up by Network Users. Any non-approved remote access services found to be in existence will be immediately removed from the network and would be consider a serious breach of this policy.

11.4.5 Remote Access to Email via Microsoft Outlook Web Access (OWA) and the College's Virtual Learning Environment; Moodle, are provided as part of the standard HR New User IT Access Request procedure and automatically configured for new network users.

11.5 Anti-Virus Security

11.5.1 Anti-virus and Anti Malware software are installed and maintained on every College Server and PC. The AV definition files are automated and checked hourly and updated when available.

11.5.2 Anti-Virus protection status reports are emailed to the Director of IT & Estates and senior IT staff to ensure that all Servers and PCs are maintained with the latest definition files.

11.5.3 Users must ensure that they are running with adequate and up-to-date anti-virus software at all times. If any user suspects that their PC is infected with a virus or malware they must inform the IT Services Helpdesk immediately.

11.5.4 If IT Services detect a machine behaving abnormally due to a possible viral infection it will be disconnected from the network until deemed safe. Reconnection will occur after the malware has been cleared.

11.6 Backup Processes

11.6.1 Backups are designed to protect systems and data in the College to ensure it is not lost and can be recovered in the event of an equipment failure, accidental or intentional destruction of data, or disaster.

11.6.2 Definitions

- *Backup* - The saving of files or data onto Network Attached Storage (NAS), magnetic tape or other offline mass storage media for the purpose of preventing loss of data in the event of equipment failure or loss or data.
- *Archive* - The saving of older or unused files onto magnetic tape or other offline mass storage media for the purpose of Disaster Recovery and releasing on-line storage capacity.
- *Restore* - The process of bringing off-line storage data back from the off-line media and putting it on an on-line storage system such as a server or SAN.

11.6.2 Backups are typically taken from Servers and SANs but are not limited to these central storage devices. Servers expected to be backed up include the file servers, Email servers and all MIS Systems.

11.6.3 IT Services are responsible for all of the College system and data backups, restoration and testing and shall carry out, record and monitor regular backups and restore testing. IT Services maintain a Backup Service Catalogue containing the procedures for backups and a Backup Calendar outlining all scheduled backups.

11.6.4 IT Services are responsible for testing the ability to restore data from backups on a monthly basis.

11.6.5 Offline backup tapes used for nightly backups are stored in the College’s on-site fireproof safes.

11.6.6 Offline backup tapes used for the monthly backups are stored off-site at Coulsdon College.

11.6.7 Annual archives are made at the end of the academic year in July (student backups) and annual year in December (staff and MIS archives). These tapes are stored off-site at Coulsdon College.

11.6.8 Users that require files restored must submit a request to the IT helpdesk and include information about the file creation date, the name of the file, the last time it was changed, and the date and time it was deleted or destroyed.

12. Compliance and Awareness

12.1 The College has established this policy to promote information security and compliance with relevant legislation, including the Data Protection Act and General Data Protection Regulations (GDPR). The College regards any breach of information security requirements as a serious matter. Any employee found to be have breached this policy may be subject to disciplinary action.

12.2 Compliance with this policy should form part of any contract with a third party that may involve access to network or computer systems or data.

12.3 To ensure that staff have a solid understanding of College security policy, procedure and good practice, all staff are provided with GDPR and Information Security training as part of the staff induction process.

13. Related Documentation and Legislation

13.1 College Policy

- Information Technology (IT) and Monitoring Policy
- Information Policy
- Business Continuity Plan
- Code of Conduct - Staff Policy
- Disciplinary Procedures
- Whistleblowing Procedure
- Safeguarding and Prevent Policy

13.2 Legislation

The College has an obligation to abide by all UK legislation and relevant legislation of the European Community. The following Laws are of particular importance in the use of IT systems and computers. This list is not exhaustive and is subject to change.

- Copyright Designs and Patents Act 1988
- The Data Protection Act 2018

- General Data Protection Regulation 2018
- The Computer Misuse Act 1990
- The Regulation of Investigatory Powers Act 2000
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- The Freedom of Information Act 2000
- Counter-Terrorism and Border Security Act 2019