Croydon College

COULSDON
SIXTH FORM COLLEGE

Croydon
University
Centre

INFORMATION TECHNOLOGY (IT) AND MONITORING POLICY
Approved by: Executive
Date approved: 22 February 2022
Strategy/Policy Responsibility: *Vice Principal Finance and Resources*
Review date: January 2024

Information Technology (IT) and Monitoring Policy

1 Introduction

1.1 Croydon College provides Information Technology (IT) resources including computing, telephone, Internet and Email access for Employees use to promote the aims of the College and to facilitate education, research and the business of the organisation.

1.2 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 Colleges 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.

1.3 There is an expectation placed on all Employees that IT equipment, systems and resources will be used in a secure, responsible, efficient, ethical and legal manner.

1.4 This policy is designed to help Employees understand College-wide expectations for the use of IT equipment, systems and associated resources and outlines what the College considers inappropriate use. Failure to adhere to these guidelines could result in disciplinary and legal action being taken.

2 Scope

2.1 This policy applies to all IT equipment and supporting technologies owned by, and used within Croydon and Coulsdon Colleges, including remote access. The policy is subject to, and in addition to UK legislation. In cases where the UK legislation has been breached by an Employee, civil and criminal sanctions may apply.

2.2 Directors, Heads of School and Line Managers have a responsibility for ensuring the implementation of, adherence to and compliance with this policy throughout their areas of functional responsibility.

3 Acceptable Use Standards

3.1 All Employees are expected to use IT equipment, Email and Internet access primarily for College business and education or research related purposes. All Employees are expected to conduct themselves honestly and appropriately when using these resources and comply with copyright, licencing rules, intellectual and other property rights, privacy and the prerogatives of others.

3.2 All Employees must read and accept the terms of this policy as part of the HR New User IT Access Request procedure before being allocated appropriate logon and password credentials for College systems. Any Employee found abusing College systems may be subject to the College's Disciplinary Procedure or other equivalent process.

3.3 Acceptable use is defined as:-

- Teaching, learning and assessment
- Research
- Personal educational development
- Administration and management of College business
- Development work and related communication
- Consultancy work while contracted at the College
- Reasonable use of IT facilities for personal correspondence and research in the Employee's own time, where not connected with any commercial activity and where such use is in accordance with this policy, is regarded as acceptable. The College reserves the right to withdraw this facility wholly or in part at its absolute discretion
- Use for other purposes may be permitted by Executive Management or the Director of IT & Estates.

3.4 Accessing, storing or transmitting unacceptable or illegal materials will be regarded as an offence that may result in the finding of gross misconduct and summary dismissal, and in the case of suspected illegal activity may result in police involvement and action. The following activities are considered an unacceptable use of IT resources:

3.4.1 Using College IT or the Internet for any illegal purpose.

3.4.2 Using online gambling sites.

3.4.3 Sending or knowingly receiving Emails that contain pornography, (defined by Obscene Publications Act 1959 or other relevant legislation), or violent, harassing, abusive, terrorist-related, drug-related, discriminatory content or material which otherwise includes unethical or illegal solicitation, inappropriate language, and/or information used to promote racism or sexism or other unlawful discrimination or hate crime.

3.4.4 Displaying, storing, archiving, distributing, editing or recording sexually explicit material using the College network or computing resources. Access to such sites are generally blocked from within College networks but if for any reason a site that contains sexually explicit or offensive material is accessed, it must be disconnected immediately and a member of the IT Services team informed.

3.4.5 Sending or knowingly receiving, storing or using copyrighted materials, videos and music without the owner's permission.

3.4.6 Distributing software or materials in violation of the licence terms and conditions.

3.4.7 Installing or downloading illegal, pirated or unlicensed software.

3.4.8 Breaching any copyright, designs, trademark or patents rights.

3.4.9 Using the network/Internet to deliberately propagate any malicious code, malware or phishing emails or web pages.

3.4.10 Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of where you are not the intended recipient or logging into a computer or account that you are not expressly authorised to access. For purposes of this section, "disruption" includes, but is not limited to port scanning, network spoofing, packet sniffing, pinged floods, and denial of service for malicious purposes.

3.4.11 Using College IT resources or Internet for personal financial gain or private commercial activity.

3.4.12 Using the network/Internet for product advertisement or political lobbying.

3.4.13 Using the College network/Internet to make unauthorised entry into other systems or communication services or resource (hacking).

3.4.14 Using another person's username and password or allowing someone else to use their credentials.

3.4.15 Storage of non-College related data or media such as personal photos, music, video etc. on the College network.

3.4.16 Installing or connecting unauthorised equipment to the College network.

3.4.17 Physical damage to any IT equipment or services.

3.4.18 Removal or relocation of any IT equipment without appropriate permission from IT Services.

3.4.19 Copying or removing any personal data defined under the Data Protection Act unless in an encrypted format as laid out in the College's Information Policy.

3.4.20 Bypassing or attempting to bypass any College IT security or firewall systems.

3.4.21 Bypassing College Internet filtering using a proxy or other services.

3.4.22 Using remote access software except where directed by IT Services.

3.3.23 Persistent or unacceptable personal use of Email including but not limited to personal messages, social invitations, jokes, cartoons, or chain letters.

3.4.24 Using College IT Systems to commit Croydon College to purchasing or acquiring goods or services without proper authorisation as laid out in the College's Financial Regulations.

4 Email Access

4.1 Employees are authorised to use internal and external Email for business reasons as described above.

4.2 Employees must not use internal or external Email to send or solicit the receipt of any offensive, defamatory or discriminatory material or any material, which may include nudity or amount to sexual, disability, racial or other harassment unless related to an individual's role within the College. This also includes the creation or transmission of defamatory, hurtful or malicious material.

4.3 An Employee who is in receipt of an inappropriate Email or attachment should immediately report this to IT Services and their line manager. The line manager should consult with the Director of HR on whether an investigation under the Disciplinary Procedure should be instigated. Inappropriate Emails include Emails containing any defamatory or discriminatory material, or any material, which may amount to any type of discrimination or harassment. This list, however, is not exhaustive and does not include junk Emails (also known as SPAM Emails), which should simply be deleted.

4.4 Email has the same legal status as a paper document for the purposes of prosecuting those who publish copyright material without proper permission or defamatory material and can be submitted in court proceedings.

4.5 Email communications are not secure. Employees must not reveal any information that is protected by the Data Protection Act 1998, the General Data Protection Regulations (GDPR) 2018 or within the confidentiality clauses in employment contracts, which they do not have authority or consent to reveal through other forms of communication.

4.6 Care should be taken with expressions used and messages should be of similar standard to memos, letters, etc. Please also be aware that automatic responses to Emails (e.g. covering holiday or "Out of the office periods") may apply to both internal and external Emails and should therefore be business appropriate, and courteous.

4.7 A disclaimer is automatically attached to all outgoing external Emails to the effect that the opinions expressed are not necessarily those of the College; the individual is therefore personally liable for the content of the Emails they send.

4.8 Only authorised Employees may send All User Emails and these are only distributed for important or strategic information. Emails to all users must not be sent to inform staff of personal activities or invites to leaving parties etc. The staff Intranet provides the facility for these types of activities.

5 Phishing

5.1 Phishing is a cybercrime in which a target or targets are contacted by email, telephone or text message by someone posing as a legitimate institution to lure individuals into providing sensitive data such as personally identifiable information, banking and credit card details, and passwords. The information is then used to access important accounts and can result in identity theft and financial loss.

5.2 Employees must make themselves aware of the dangers of Phishing and report any such Emails to IT Services immediately.

Please see the following link for more information on Phishing

http://en.wikipedia.org/wiki/Phishing

5.3 Employees must use extreme caution when opening Email attachments received from unknown senders, as they may contain viruses, Email bombs, or Trojan horse code.

5.4 All account details including passwords and bank details must be kept secured and never shared with any other person or on any website. The College, banks or finance companies will never ask for your password for any purpose.

5.5 If an Employee becomes aware that any network account or password has been compromised the password must be changed immediately and IT Services Informed. Failure to do so could result in suspension of network and email access and disciplinary procedures.

6 Internet Access

6.1 Employees may be authorised to use the Intranet and the Internet for business purposes.

6.2 College Internet access is provided by JISC over the JANET network (Joint Academic Network). JANET is the network dedicated to the needs of research and education in the UK. All College internet users must comply with the JANET Acceptable Use Policy (AUP) available from:
https://community.jisc.ac.uk/library/acceptable-use-policy

6.3 Employees should be aware of the time they spend on the Internet, be clear about their objectives when accessing the Internet, be able to account for the time spent on the internet and be able to provide reasons why they visited any particular site during their working hours.

6.4 Employees must not access any inappropriate site or any site providing pornography, or any other unsuitable material on the Internet. Employees must not download any pornographic or unsuitable material from the Internet. Breach of this condition in any way may render Employees liable to summary dismissal for gross misconduct. Employees must immediately notify IT Services if they accidentally enter or receive any web site material which is inappropriate. Inappropriate sites include material which may amount to discrimination or harassment or include nudity, unless related to an individual's role within the College. This list, however, is not exhaustive.

6.5 The prevention of inappropriate use of the Internet is aided by the use of web filtering systems. These systems log detailed usage of websites by all users and enable the blocking of inappropriate websites. Employees requesting the unblocking of web sites for legitimate business or curriculum use must obtain consent from their line manager before contacting IT Services.

7 Network and Systems Access

7.1 New Employees who require access to the College IT MIS systems, Email and Internet, in order to carry out their duties, are required to complete a HR New User IT Access Request procedure on Induction and receive a copy of this Policy and accept its conditions.

7.2 Systems and information at different levels are password protected. Employees are responsible for the activities undertaken using their personal login and password, and as such, it is the individual's responsibility to maintain their own password security. Employees must not reveal passwords to anyone, and if someone gains knowledge of a password, the user must change his or her password immediately. Please see the College's Information Security Policy for further information on the College's Authentication and Password Policy.

7.3 Employees should also always ensure that systems are closed down or locked if the computer is left unattended for any length of time. Employees must not attempt, alone or with others, to gain access to data or systems to which they have not been given authorised access.

7.4 Employees must not allow any student to use their network login and password credentials. This is a breach of College's Information Security Policy and the College Disciplinary Procedure or other equivalent procedure could be invoked.

7.5 Employees must be aware of the risks of computer viruses and take appropriate precautions to avoid the possibility of viruses or malware entering any college computer or network. Employees must not disable or change the configuration of any Anti-virus or security setting on College computers or IT systems.

7.6 Employees must not, except with prior authority from IT Services, load or download any software onto a College computer.

7.7 Employees are expected to take responsible care when working with files created on the College systems and on Microsoft 365, Teams and OneDrive. Regular backups taken by the College are designed for Disaster Recovery but will not be generally available for recovering staff files without a clear business case.

8 Using Your Personal Devices to Access College Systems

8.1 The College allows you to use your personal device to access College Wi-Fi and systems. Employees must only use a list of approved and tested Operating Systems and applications when accessing College Systems from their own personal devices. The list of currently supported versions is regularly updated on the IT Services Page on the College Intranet, “Approved Apps and OS for your Personal Device”.

8.2 Users Accessing Remote Desktop Services must read and accept a Remote Desktop Access Policy when first accessing the service and when the policy is updated from time to time.

8.3 For security reasons devices running older software updates can present a security risk and must not be used to access College Systems. The auto-update feature for all software must be enabled to automatically download and install latest security updates.

8.4 All Staff employees, agency staff and other external stakeholders are expected to use their device in an ethical manner. Using your device in ways not designed or intended by the manufacturer is not allowed. This includes, but is not limited to, “jailbreaking” your iPhone or “rooting” your android device.

8.5 Devices must have anti-malware software, such as Windows Defender installed and always kept up to date.

9 College Telephones

9.1 Employees are authorised to use College telephones for external and internal use. Such authorisation extends primarily to use for the purpose of their work and incidental needs of the business.

9.2 Employees may use College telephones for urgent personal calls only. Personal calls should always be kept to a minimum and where possible made outside of office hours. An Employee found making unauthorised calls or abusing this facility may be subject to the College’s Disciplinary Procedure or other equivalent procedure.

9.3 International calls must only be made for identifiable business purposes, kept to a minimum and arranged through the College Front of House team for audit purposes.

9.4 Croydon College reserves the right to monitor the destination, volume and duration of all incoming and outgoing calls to the College phone system to support the business interests of the College and to investigate complaints.

9.5 Employees should be aware that their voicemail messages may need to be checked or redirected if they are absent, particularly if the absence is unexpected. This would be approved by Executive Management or the Director of IT & Estates.

10 Mobile Devices

10.1 Where a mobile device such as a mobile/smart phone, tablet, or broadband dongle has been provided to an Employee, the Employee has responsibility for managing and protecting the mobile device and the data contained within it.

10.2 All Mobile devices are centrally managed and monitored via a Mobile Device Management (MDM) system. Staff must not attempt to re-configure any of the MDM features.

10.3 Where available, all mobile devices must be secured with a PIN at all times and locked when not in use. Where a PIN or password has been configured this function must not be disabled.

10.4 Calls from a mobile/smart phone should be kept to a minimum and used only when a more cost effective fixed line phone is not available. Devices should not be used for personal calls or personal SMS texts where costs would apply.

10.5 In the event that a mobile device is lost or stolen, the Employee must immediately inform IT Services to prevent unauthorised access.

10.6 Personal information, as defined by the GDPR and College Information Policy must not be stored on any mobile device.

10.7 Mobile devices no longer required must immediately be returned to IT Services for redistribution or cancellation of the contract.

11 Social Media

11.1 The College's official social media activity is managed by the Marketing Department who will involve College Employees across the organisation in order to use Twitter, Instagram, Facebook, LinkedIn and other developing social communication tools for the benefit of the College and its students.

11.2 To this end, Employees may use personal social media accounts to interact with and promote the College's social media campaigns, but online activities must not interfere with work performance.

11.3 Employees must share information carefully and keep in mind that all posts are potentially visible by all on-line users. Employees should not reveal any information that compromises Croydon College policies, its public position, the Data Protection Act or GDPR.

11.4 Employees should seek guidance before participating in social media when the topic being discussed may be considered sensitive (e.g. a crisis situation, intellectual property, issues which may impact on the College's reputation, commercially sensitive material). Social media activity around sensitive topics should be referred to the Marketing Department.

11.5 All posts on Social Media sites, such as Twitter, must be in line with the College's values and all relevant policies and procedures. If an Employee's use of social media is considered to be derogatory, discriminatory, bullying, threatening, defamatory, offensive, harassing, creating legal liability for the College or bringing the College into disrepute then the College may take action under the Disciplinary Procedure (Staff). This may include comments, videos, or photographs, which have been posted on social media sites about the College, students, work colleagues or managers.

11.6 The use of social media in a personal capacity is only permitted outside of normal working hours in line with Paragraph 3.3 above.

11.7 Setting up social media accounts, groups or pages in the name of Croydon or Coulsdon College is prohibited unless express permission has been given by the Executive Group through the Marketing Department. This applies to all social media platforms.

12 Monitoring

12.1 This Policy aims to provide an appropriate balance between respecting an Employee's privacy whilst allowing the necessary monitoring and scanning required to fulfil its business needs and legal obligations. By using College IT systems, equipment or resources, Employees consent to the processing of any personal data which may be revealed by any monitoring carried out in accordance with this policy.

12.2 The College carries out a range of monitoring to ensure that its IT systems are operating efficiently and effectively. Such monitoring is not, in general, person specific but an Employee's personal data may be accessed as part of this procedure. These monitoring procedures are in place to:

- Maintain effective IT Systems
- Comply with regulatory and statutory obligations including our Prevent Duty
- Prevent or detect unauthorised use, criminal activity or other threats to College IT systems
- Ensure compliance with College policies and procedures
- Identify IT usage and staff training

12.3 In order to prevent the abuse of systems and equipment, the College reserves the right to access, review, and monitor the use of computers, telephones, contents of Emails and the use of the Internet but only where authorised by the Head of Human Resources and where it is fair and proportionate to do so.

12.4 The College will respect Employee privacy in accordance with the Human Rights Act 1998, the Data Protection Act 2018 and the GDPR 2018 and will act in accordance with its obligations under UK legislation.

12.5 Monitoring may take place as required to meet our operational and legal requirements. Employees who have concerns about privacy should not use College IT equipment and resources for personal use. Confidentiality and privacy of telephone calls, Emails and Internet access should not be assumed.

12.6 This policy recognises the difference between:

- Usage logging – collecting data about how and when a person used College IT systems; and
- Content inspection – viewing information held within business or personal files, Emails or voicemails

12.7 Usage Logging

- The College carries out usage logging on a regular basis to improve the performance of its IT systems and to help identify and investigate prohibited activity or misuse.
- None of this data contains the content of the communications or files and is restricted to the day-to-day administration of College IT Systems and any potential Freedom of Information (FOI) requests.

12.8 Content Inspection and Authorised Access

12.8.1 Content inspection may occur:

- To fulfil College business when a user is unexpectedly absent or is on leave
- To satisfy GDPR subject access or Freedom of Information requests
- Where the College has reason to believe that a breach of this policy has occurred
- At the request of law enforcement and Counter Terrorism officers

12.8.2 Content inspection involves viewing information within:

- Business and/or personal electronic files or documents
- Business and/or personal Email messages
- Telephone and mobile phone voicemail messages
- Internet usage logs
- IT Systems access logs
- Print System logs and reports
- ID-Card, security barrier, CCTV and access control logs
- Business or personal information displayed on computer screens

13 Compliance and Awareness

13.1 It will be the responsibility of all College Employees to ensure the security of College IT systems as outlined in this and other College policies.

13.2 Following a breach of this or any other College Policy or under exceptional circumstances, the Director of HR may, with no notice, request IT Services to disable access to an Employee’s College IT systems, Email and Internet.

13.3 This Policy will be provided and referenced as part of the HR New User IT Access Request procedure and is available on the College staff Intranet.

14 Related Documentation and Legislation

14.1 College Policy

- Code of Conduct Policy (Staff)
- Disciplinary Procedure (Staff)
- Financial Regulations
- Information Security Policy
- Information Policy
- Safeguarding and Prevent Policy
- Whistleblowing Policy

14.2 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 Computer Misuse Act 1990
- The Human Rights Act 1998
- The Data Protection Act 2018
- General Data Protection Regulation 2018
- Regulation of Investigatory Powers Act 2000
- The Telecommunications (Lawful Business Practise) (Interception of Communications) Regulations 2000
- Freedom of Information Act 2000
- Counter-Terrorism and Border Security Act 2019