Reference: IT_01

Document title: IT and Data Security Policy

Developed by: Paul Cutten, IT Systems & Services Manager

Date developed: February 2021

Date of approval: 24th February 2021

Committee approving: SLT

Date of equality analysis: January 2021

Date becomes effective: March 2021

Reviewed by: N/A

Review date: Updated Nov 2021 Version: 2.0

Date of next review: March 2024

Please contact us on 01904 770132 or email us at qi-admin@yorkCollege.ac.uk if you would like this document in an alternative format

To ensure version control, please do not print this document – as tomorrow it could be out of date.

Please contact the IT Helpdesk at ithelpdesk@yorkcollege.ac.uk if you have any questions about all or part of this document.

York College IT and Data Security Policy

Contents

1 Acceptable Use Regulations

1.1 Scope

Section 1 defines the acceptable use regulations that apply to anyone using the IT facilities provided or arranged by York College.

The term IT facilities include:

- IT hardware that York College provides, such as but not limited to PCs, laptops, tablets, smartphones, 4G/5G internet routers, and printers.

- Software that the College provides, such as but not limited to operating systems, office application software, and web browsers. 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 York College 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, on campus WiFi, connectivity to the internet from College PCs.

- Online services arranged by the College, such as Microsoft 365 or library e-books.

- IT credentials, such as the use of your College login, or any other token (email address, ID card, multi-factor authentication card) issued by York College to identify yourself when using IT facilities. For example, you may be able to use drop in facilities or WiFi 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.

The scope includes, but is not limited to:

- Visitors to York College's website, and people accessing the College's online services from off campus.

- External partners, contractor and agents based onsite and using York College's 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 WiFi networks.

1.2 Behaviour

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 (see section 1.8 Goverance), but it is also subject to general laws and regulations such as the College's policies and code of conduct.

- Real world standards of behaviour apply online and on social networking platforms, such as but not limited to Facebook, WordPress, Instagram, and Twitter.

- You must not cause needless offence, concern, or annoyance to others. You must not harass people or discriminate against people based on protected characteristics (age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex, sexual orientation).

- 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.

- 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.

- When using shared spaces, remember that others have a right to 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.

- Use resources wisely. Do not waste paper by printing more than is needed, or by printing single sided when double sided would do. Don't waste electricity by leaving equipment needlessly switched on.

- You must not use IT facilities to attempt to radicalise or encourage extremist views or behaviours in others, or to distribute material related to such views or behaviours.

1.3 Intended Use

- The IT facilities are provided for use in furtherance of the mission of York College, 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 (if 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 IT facilities for non-institutional commercial purposes, or for personal gain, such as running a club or society, requires the explicit approval of the IT Systems & Services Manager.

- Staff 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.

- 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).

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

- 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.

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

1.4 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 usually in the form of a username and password, but other forms of IT credentials may be used, such as an email address, an ID card, or some other form of security device.

In protecting and maintaining the security of their credentials users shall comply with the policy regulations set out in section 2.5 User ID/Passwords.

1.5 Infrastructure

The IT infrastructure consists of all the underlying resources that make IT function. It includes servers, the network, PCs, 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 integrity of the IT infrastructure such as but not limited to:

- Damaging, reconfiguring, or moving equipment.
- Loading harmful software onto College owned equipment or circumventing any measures in place to prevent the loading of software onto such equipment.
- Reconfiguring or connecting equipment to the network other than by approved methods.
- Setting up servers or services on the network without permission. Examples would include games servers, file sharing services, IRC servers or websites.
- Deliberately or recklessly introducing malware.
- Attempting to disrupt or circumvent any other IT security measures designed to safeguard the security of the IT infrastructure e.g., antivirus software, firewalls, web filters, and spam filters.

1.6 Information

If you handle personal, confidential, or sensitive information, you must take all reasonable steps to safeguard it and should be aware of and observe the requirements of the General Data Protection Regulation. Care should be taken regarding removable media, mobile and privately-owned devices.

- You must not infringe copyright or break the terms of licences for software or other material.
- When sending protected information electronically, you must use a method with appropriate security. The recommended method is to share the data via your College OneDrive, Teams, or a SharePoint site. Please contact ithelpdesk@yorkcollege.ac.uk for further details.
- You must not attempt to access, delete, modify, or disclose information belonging to other people without their permission.
- You must not create, download, store or transmit unlawful material, or material that is indecent, offensive, threatening, discriminatory, liable to radicalise or is considered extremist. Valid activities involving the use of such material should be discussed and agreed with a Strategic Leadership Team (SLT) member in advance of access or usage.

See section 3 – Data Security for more in-depth guidance.

1.7 Monitoring

- York College may monitor and record the use of its IT facilities for the purposes of:
    - The effective and efficient planning and operation of the IT facilities.
    - Detection and prevention of infringement of these regulations.
    - Investigation of alleged misconduct.
    - Any other lawful purpose as may arise or be imposed upon the College.
- York College will comply with lawful requests for information from government and law enforcement agencies.
- You must not attempt to monitor the use of the IT without the explicit permission of the IT Systems & Services Manager. This would include:
    - Monitoring of network traffic.
    - Network and/or device discovery.
    - WiFi 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.

1.8 Governance

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.

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

- General Data Protection Regulation
- Obscene Publications Act 1959 and Obscene Publications Act 1964
- Protection of Children Act 1978
- Police and Criminal Evidence Act 1984

- Copyright, Designs and Patents Act 1988
- Criminal Justice and Immigration Act 2008
- Computer Misuse Act 1990
- Human Rights Act 1998
- Regulation of Investigatory Powers Act 2000
- Prevention of Terrorism Act 2005
- Terrorism Act 2006
- Police and Justice Act 2006
- Freedom of Information Act 2000
- Freedom of Information (Scotland) Act 2002
- Equality Act 2010
- Privacy and Electronic Communications (EC Directive) Regulations 2003 (as amended)
- Defamation Act 1996 and Defamation Act 2013

- 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, and 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 must abide by the regulations applicable to any other organisation whose services you access such as Jisc, including use of the College's "Janet" internet connection.

- When using the ‘eduroam’ WiFi network at College or another institution, you are subject to both the regulations of York College and the institution where you are accessing services.

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

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.

General College regulations

You should already be familiar with York College's general regulations and policies. These are available at www.yorkcollege.ac.uk

Third party regulations

If you use York College 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).

In some cases, the service is so pervasive that you will not even know that you are using it.

Two examples of this would be:

- **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 York College you will be using Janet, and subject to the Janet Acceptable Use Policy, https://community.ja.net/library/acceptable-use-policy and the Janet Security Policy, https://community.ja.net/library/janet-policies/security-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.

- **Using Chest agreements**
  Eduserv is an organisation that has negotiated many deals for software and online resources on behalf of the UK 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 https://www.chest.ac.uk/user-obligations/

There will be other instances where York College has provided you with a piece of software or a resource. Users shall only use software and other resources in compliance with all applicable licences, terms, and conditions.

1.9 Authority

- These regulations are issued under the authority of the IT Systems & Services Manager who is also responsible for their interpretation and enforcement, and who may also delegate such authority to other people.

- 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 via the IT Helpdesk ticketing system, for the attention of the IT Systems & Services Manager.

- 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 a College website; a self-service kiosk in a public area; or an open WiFi 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 ithelpdesk@yorkcollege.ac.uk

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

1.10 Infringement

- Infringing these regulations may result in sanctions under the College's disciplinary processes. Offending material may be removed, and York College will not be liable for any loss because of such removal.

- Depending upon the nature of the infringement, you may also face criminal charges or civil action brought by other parties. Information about infringement may be passed to appropriate law enforcement agencies, and any other organisations whose regulations you have breached.

- York College reserves the right to recover from you any costs incurred because of your infringement.

- You should inform the IT Helpdesk if you become aware of any infringement of these regulations.

2 IT Security

2.1 Scope

Section 2 defines the IT Security regulations for York College and sets out how the College approaches protecting the confidentiality, integrity, and availability of the network. The IT Security regulations apply to all business functions and information contained on the network, the physical environment and relevant people who support and are users of the network.

The network is a collection of communication equipment such as servers, computers, printers, access control and CCTV systems connected by cables or wireless devices. The network is used to share data, software, and peripherals such as printers, internet connections and data storage equipment.

To ensure the security of the College's network and systems the College will:

- Ensure Availability - Ensure that the network is available for users.
- Preserve Integrity - Protect the network from unauthorised or accidental modification.
- Preserve Confidentiality - Protect assets against unauthorised disclosure.

This policy applies to all networks managed by the College used for:

- The storage, sharing and transmission of College and non-College data and images.
- Printing or scanning non-College or College data or images.
- The provision of internet systems for receiving, sending, and storing non-College or College data or images.
- To support the College Building Management, Security and CCTV systems.

The College information network will be available when needed and can be accessed only by legitimate users. The network must also be able to withstand or recover from threats to its availability, integrity, and confidentiality. To satisfy this, the College will undertake the following:

- Protect all hardware, software, and information assets under its control. This will be achieved by implementing a set of well-balanced technical and non-technical measures.

- Provide both effective and cost-effective protection that is commensurate with the risks to its network assets.

- Implement the IT Security policies in a consistent, timely and cost-effective manner.

- The College will act in compliance with its legal requirements and co-operate with investigating parties acting under UK legislation or court order. This includes the disclosure of any data or activity on College systems when legally instructed to do so.

2.2 Risk Assessment and audit

The College is responsible for ensuring that appropriate risk assessment(s) are carried out in relation to all the business processes covered by this policy. The risk assessment will identify the appropriate countermeasures necessary to protect against possible breaches in confidentiality, integrity, and availability.

2.3 Physical & Environmental Security

- Core network equipment will be housed in a controlled and secure environment.

- Critical or sensitive network equipment will be housed in an environment that has a monitored temperature, backup power supply and will be protected by fire suppression systems.

- All visitors to secure network areas must be authorised by the IT Systems & Services Manager.

- Entry to secure areas housing critical or sensitive network equipment will be restricted to those whose job requires it.

- The IT Systems & Services team will ensure that maintenance contracts are maintained and periodically reviewed for all essential network equipment and services.

2.4 Access Control to the Network

- Access to the network will be via a secure log-on procedure, designed to minimise the opportunity for unauthorised access. Remote access will be via secure Multi-Factor Authentication where supported.

- There must be a formal, documented user registration and de-registration procedure for access to the network. Remote access to data will be secured with the College's Mobile Management system. This will require the user to enrol their College account

for Multi-Factor Authentication. Policies from the Mobile Management system will ensure segregation of personal and College data.

- The departmental manager must approve user access prior to being processed by the IT helpdesk.

- Access rights to the network will be allocated on the requirements of the user's job, rather than on a status basis.

- Administrator permissions will not normally be allocated to any day-to-day user account (including IT team members) and not without written permission from the IT Systems & Services Manager. A central record will be kept of privileged accounts.

- Access will not be granted to members of staff until Human Resources have given the go ahead to the IT Systems & Services team to generate the user's account.

- All users to the network will have their own individual user identification and password.

- User access rights will, upon notification from departmental managers, be immediately removed or reviewed for those users who have left the College or changed jobs.

- Accounts which remain unused for six months become liable to be disabled.

- No shared accounts will be created, except where absolutely necessary, and under the condition that a list is kept of the users of the account, and that they are jointly responsible for any action taken using the account.

- Accounts should not be re-used, except where absolutely necessary, and under the condition that a record is kept of the users of the account.

- Lists of users and their data must not be available to anonymous users or, where possible, to other users and systems administrators.

2.5 User ID/Passwords

- Access to any network connected device must be via a logon process that identifies and authenticates the user.

- Authorised users are allocated a username and password and the user is responsible for protecting the confidentiality of their College IT credentials. To that end users should comply with the following:

- Users must not allow anyone else to use their IT credentials. Nobody has the authority to ask an individual for their password.
- An ID card or other security hardware should not be shared with others. If lost, users should report the matter to IT immediately.
- Users should refrain from using the same password(s) for College and personal accounts.
- Users must inform ITSS immediately if they suspect someone else of using their username/password.
- Users should not use their College credentials to log in to websites or services they do not recognise, and do not show the padlock symbol.
- Users should not attempt to disguise or hide their real identity when using the College's IT facilities. However, it is acceptable not to disclose identity if the system or service clearly allows anonymous use (such as a public facing website).
- Users should not attempt to obtain, usurp, borrow, corrupt, or destroy someone else's IT credentials.

- In some cases, it may be necessary for others to access IT facilities on an individual's behalf (e.g., a personal assistant or carer) or to gain access to another's account or information (e.g., a manager in the case of staff who are absent). In such cases users should liaise with a manager first who can raise the request with the IT team.
- Devices must be locked when logged in and left unattended.
- Users should log out when finished using a computer.
- With regards to user passwords: -
    - Passwords should be committed to memory and not written down.
    - Credentials may be stored in a secure password vault, such as 1Password, LastPass or KeePass.
    - Passwords should not be easy to guess e.g., names of relatives or pets.
    - College will enforce regular password changes.
    - College will maintain a blacklist of known weak/compromised passwords and block their use.

- Passwords should not contain the user's network account name or parts of the user's full name that exceed two consecutive characters.

- They should not be reused i.e., numbers added or increased on your previous password.

- Passwords should be at least 8 characters in length and contain characters from each of the following categories:
  i. English uppercase characters (A through Z)
  ii. English lowercase characters (a through z)
  iii. base 10 digits (0 through 9)

- Use of a passphrase is recommended, especially if it is nonsense e.g. *I love t0wel grass windows*

2.6 Remote Access

Remote Access refers to any technology that enables the College to connect users in geographically dispersed locations. Remote access implementations that are covered by this section include, but are not limited to, dial-in modems, ISDN, DSL, VPN, RDP, and cable modems.

- The IT Systems & Services team is responsible for providing clear authorisation mechanisms for all remote access users.

- All remote access users are responsible for complying with this policy and associated standards. They must safeguard corporate equipment and information resources and notify the College immediately of any security incidents and/or breaches.

- The IT Systems & Services team is responsible for ensuring that the Remote Access infrastructure is periodically reviewed, which could include but is not limited to independent third-party penetration testing.

- It is the responsibility of College staff, contractors, students, and consultants with remote access privileges to the College's corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection.

- All devices that are connected to York College internal networks and/or resources via remote access technologies must use up-to-date anti-malware software.

- Personal equipment that is used to connect to York College owned networks and/or access College data must have the latest security updates for the device installed.

- Only College approved remote access methods may be used.

- Security settings enforced on corporate and personal devices may include (but are not limited to) requiring multi-factor authentication, applying a PIN to apps that access corporate data, and restrictions on copy/cut/paste.

2.7 Wired Network

- All network devices that constitute part of the York College campus network shall be of a make and design identified, approved, and deployed by the IT Systems & Services (ITSS) team.

- Users are strictly prohibited from connecting any network device to the College network without prior permission of ITSS. If such devices are found, then ITSS reserves the right to render such devices dysfunctional.

- The use of network scanning software and/or hardware is strictly prohibited, unless used by or in conjunction with ITSS.

- The use of network hubs/switches anywhere in the College's network is strictly prohibited, unless used legitimately as an aid to troubleshooting and traffic analysis, and permission is given prior to use by ITSS.

- The use of network management tools is strictly prohibited, other than those deployed by ITSS.

- Any attempt to configure, physically alter or remove any of York College network infrastructures by any user is strictly prohibited, unless permission is granted from ITSS.

2.8 Wireless Network

The College has deployed a wireless network across its premises which is for the use of staff, students, and authorised representatives only, to connect College owned and Personally owned (BYOD) IT equipment to the network.

The wireless network security standards are as follows:

a) Access Layer: Users will connect to WiFi via Access Points (APs), which will provide the 802.11g/n/ac connection standard for the client devices.

b) Service Set Identifier (SSID): The SSID for the staff and student WLAN access is secured from inappropriate access.

c) The BYOD SSID (eduroam) for staff and students and authorised visitors will be broadcast for ease of access. Users will connect with their College username and password. For visitors whose home institution does not provide eduroam credentials, access will be granted via the IT helpdesk.

d) Encryption: The wireless networks will utilise WPA2 AES (Advanced Encryption Standard) level of encryption.

e) Authentication: Various flavours of 802.1x Extensible Authentication Protocol (EAP) are used for secure authentication to the College wireless networks.

- All APs shall be of a make and design identified, approved, and deployed by ITSS.

- Users are strictly prohibited from installing their own APs within the network. If such devices, considered as ‘rogue’ APs are discovered, ITSS reserves the right to render such devices dysfunctional throughout our estate.

- Users shall take full responsibility for the security of their mobile computing hardware including physical devices and data stored on them, both on and off the College's campus and sites.

- Users shall never assume complete privacy when using the wireless service. It is the responsibility of the user to ensure their privacy and the protection of privileged information and/or intellectual property. The ITSS team makes no guarantees as to the security of the data traversing the wireless network.

- Attempts to bypass security or to damage the wireless service passively and/or actively are strictly prohibited.

- The use of ‘wireless packet sniffers’ is strictly prohibited, unless used by or in conjunction with the IT Systems & Services team.

- Any attempt to physically alter or remove APs by any user other than the IT Systems & Services team is strictly prohibited.

- Users must ensure their personal devices have the latest security updates installed before connecting to the College WiFi network.

- Users are responsible for ensuring sufficient anti-malware software is installed, running and up to date on their personal devices while using the College WiFi network.

2.9 Telephone Usage

Voice and other communications which occur over College telephony devices may be logged for a variety of regulatory reasons.

Call statistics via desk phones and computer based soft phone using the College's telephony infrastructure is logged for legal, system integrity, budgeting, and other related reasons, for example as part of disciplinary procedures.

Information which is logged contains at least:

- Source device
- Destination number
- Duration of call

Other information about calls may be logged as available or required. Information in these logs will be held securely and made available only in accordance with College policies.

The content of live calls is not monitored or recorded; however, voicemail messages are stored securely within the telephone system and can be made available to the Strategic Leadership Team upon request for the reasons stated above.

- In making use of College landline and mobile telephones all users are expected to act responsibly and keep costs to a minimum.

- When making or receiving any calls, internal or external, staff should aim to be pleasant, informative, helpful, and brief.

- Phones are provided for college related use. While the College recognises that occasional personal use may be necessary, this should be kept to a minimum.

- If a College mobile phone is lost, then it must be reported to a line manager and to the IT helpdesk as soon as possible.

- Information must never be given out over the phone unless it is absolutely clear who it is being given to and that they are entitled to the information.

- Care must be taken to ensure that conversations involving confidential and/or personal information cannot be overheard.

- College mobile phones must be kept secure at all times, and out-of-sight whenever possible.

2.10 Internet Usage

- In any access or use of the internet, staff and students are expected to act in a professional, business like and ethical manner and always remember that you are a representative of the College.

- The College logs all internet access. At any time, the College at its sole discretion, reserves the right to monitor internet log files and internet access using the College's IT network and equipment.

- The College employs a filtering system to prevent access via the College IT systems to materials deemed unsuitable or inappropriate. Examples of material which are filtered are those which are:

    - Pornographic
    - Online gambling
    - Online games or computer game related
    - Hatred or intolerance
    - Violence
    - Incitement to extremism
    - Threats to the security of the service or stored data

- Additionally, the filtering system records the occurrence of words and terms which are related to the above categories and may partially or completely block access to a web page based on its score.

- If a student or staff member needs access to a resource which is blocked for reasons relating to College business or educational purposes, access may be restored on a limited or general basis.

  Requests for access should be made through the IT Helpdesk, by the curriculum Head or Professional Services manager on behalf of the request originator. Each case will be reviewed independently based on the reasons provided by the requesting party.

- Users will not attempt to circumvent security and filtering measures via VPN or any other means.

- The internet facilities must not be used to attempt to radicalise or encourage extremist views or behaviours in others, or to distribute material related to such views or behaviours.

- Users should not broadcast any information to bulletin boards or public newsgroups or persons that are not directly associated with the College.

- The College communications network should not be used to sign up with websites or organisations that offer rewards, monetary or otherwise, for surfing the internet.

- Inappropriate use of College IT services including internet and email usage may be grounds for referral under the governments PREVENT strategy, and may be submitted as part of a referral, or requested by investigating parties.

2.11 Email Usage

- Email sent, received, or stored on College or provided cloud systems will be monitored periodically and is subject to inspection at any time. Prudent judgement should be exercised when composing messages.

- Whilst it is accepted that users may need to send personal messages from time to time, they should respect the primary purpose of the email system and keep personal use to a minimum. Use of the email system for personal messages is subject to the College's right to monitor the system for its legitimate business purposes, and by choosing to use the College's email system to send a personal message they consent to the College monitoring such messages (including when it is sent using a computer off-site). When users send a personal email, they must make clear that it is not associated in any way with the College.

- All email messages leaving the College should be legal, decent, honest, and appropriate to their recipient.

- Users are prohibited from using the College network to:

    - Send, receive, solicit, print, copy, or reply to text or images that are disparaging or defamatory to others based on their race, gender, disability, sexual orientation, age, ethnicity, religious beliefs, gender identity, marriage/civil partnership status, pregnancy/maternity/paternity status.
    - Spread gossip, rumours, or innuendos about staff, students, clients, suppliers, or other outside parties.
    - Send, receive, solicit, print, copy, or reply to:
        (i) sexually oriented messages or images
        (ii) messages or images that contain foul, obscene, or adult-oriented language.
        (iii) messages or images that are intended to alarm others, embarrass the College, negatively impact staff/student productivity, or harm staff/student morale.

Messages should not:

- Slander, defame, infringe staff privacy, contravene data protection legislation, reveal trade secrets, contain pornography, illegally discriminate, blaspheme, infringe

copyright, breach confidence, transmit malicious executable software or establish inadvertent contracts.

- College staff will not respond to or contact representatives of the "Media" by email. All such contact or response is to be via the College marketing department.

- Email messages leaving the College will have the following statement appended:

> This email and any attachments are confidential and intended solely for the use of the individual or entity to whom they are addressed. This email represents the personal views of the sender and is therefore not necessarily the views of York College. The author has no authority or delegation to bind the College by this email and York College accepts no responsibility whatsoever for its contents. Please note that any email sent to addresses at York College may be monitored.

- Good etiquette precludes "spamming" (the sending of unsolicited messages which provoke complaints from the recipients), "shouting" in all caps and "flaming" with unconsidered response. Messages from the College should generally be of conventional punctuation and case.

- Users must not create email congestion by sending trivial messages, forwarding 'chain letters' or unnecessarily copying emails.

- Retention of email - individual users may, from time to time, be required to either delete or archive some messages from their email storage depending on the amount of storage available and their proportionate usage.

- Users should be aware that once email leaves the College, unless encrypted, ordinary internet email is not a secure channel. Users cannot be certain who sent or received a message, or that any message was sent or received.

- Users must not intercept or read another users' email messages unless specifically authorised to do so. When permission has been given, care must be taken to ensure that third party personal data is not compromised.

- Where a clearly identified issue arises, for example in the case of long-term absence, in consultation with the HR Manager and/or a member of the Strategic Leadership Team (SLT), email access may be delegated to a member of staff's line manager.

- When a staff member leaves the employment of the College, at the discretion of the College, their email account may be disabled/deleted or delegated to their line manager.

- Email messages created and transmitted on College computers are the property of the College. The College reserves the right to monitor all email transmitted via the

College's computer system. Staff have no reasonable expectation of privacy when it comes to business and personal use of the College's email system.

- The College reserves the right in accordance with its legal and audit obligations to monitor, inspect, copy, review, and store at any time and without notice all usage of email, and all files, information, software, and other content created, sent, received, downloaded, uploaded, accessed, or stored in connection with staff usage. The College reserves the right to disclose email data and usage to regulators, the courts, law enforcement, and other third parties as required by UK law without the consent of the staff/student. This includes referrals or investigatory requests made under the PREVENT strategy.

College notices should normally be sent as a news post via the Staff and/or Student Portal. Where email is the more appropriate medium the following applies:

- Each notice will be assessed for its relevancy to College business. Notices which do not relate to College business will not normally be sent.

- Notices which only publicise leaving parties or gift collections / card signings for members of staff leaving College employment will normally be sent.

- Other personal announcements will not be sent except in exceptional circumstances and will require authorisation by a member of SLT.

- The College notice system includes an address which can be used for messages to be sent to all students, however all messages using this service should be relevant to the majority of students.

- Messages to tutors to relay to their students may also be sent, however other methods of notifying students exist (i.e., Blackboard, the Student Portal, digital signage, etc).

- Messages only for students on particular courses or in particular Curriculum Areas can be sent using the appropriate group in the email address book or other College communication platforms. Please exercise caution using these groups as most are not moderated and mistakenly sent or phrased messages may be damaging and difficult to retract later.

- You should check your notice for errors before submitting it and ensure that what you have sent is presented as you want it to be read.

- We will not normally proofread notices fully before sending them, however if we do spot problems, we will refer the problem back to the originator which will mean a delay in sending.

- Attachments and embedded images can be included in notices; however, they should be of an appropriate size and not contain copyrighted material which you have not been given permission to distribute.

- Notices themselves should not normally be sent as attachments, particularly if they only include text message as this will result in an extra step before users can view the message. Notices received in this form will be returned to the sender for reformatting. The exception to this is notices which contain complex layouts (i.e., calendars or tables) which would not or do not convert well into an email document.

- Executable files should not normally be distributed via College notices. Please contact ITSS if you need to distribute files of this type.

- Text for publication should be set out in a minimum 11pt Arial or Calibri font. Notices which differ from this to the point of potentially causing difficulty to readers will be returned to the sender for reformatting.

- Notices which appear to be controversial or use language or phrasing which seems inappropriate or likely to cause offence may be require additional authorisation before being sent or be referred to the originator for clarification or rewording.

2.12 Third Party Access Control to the Network

- The IT helpdesk is responsible for ensuring all third-party access to the network is logged.

- Access to the internet may be provided for guests or College employed contractors via the IT helpdesk.

2.13 Malicious Software

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 from people you do not know or inserting media that have been created on compromised computers.

- The IT Systems & Services team will ensure that measures are in place to detect and protect the network from viruses and other malicious software.

- Users shall not attempt to disrupt or circumvent IT security measures.

- When checking emails, users should not automatically open attachments without verifying with the sender the nature of the attachment.

- Do not automatically click on website links that may be embedded in an email without checking with the sender the reason/purpose of the link.

2.14 Change Control

- The IT Systems & Services team is responsible for ensuring that appropriate change management processes are in place to review changes to the network, IT infrastructure, and software.

- The IT Systems & Services team is responsible for ensuring that selected hardware or software meets agreed security standards.

- ITSS will provision a staged automatic rollout of security updates for managed software on college owned devices within 14 days of release.

2.15 Unauthorised software

- Use of any non-standard software on College equipment must be approved by the helpdesk before installation.

- All software used on College equipment must have a valid licence agreement - it is the responsibility of the user of non-standard software to ensure that this is the case.

- Users must not copy, or attempt to copy, any College licensed software for private use.

- Users must not attempt to install any software on the hard disk of a computer or the College network without first obtaining permission to do so from the IT Systems & Services Manager. This includes, but is not limited to, screensavers, ‘desktop wallpaper’, software updates (both manually installed and automatically downloaded and self-installing), file un-packers (e.g., PKZip, WinZip, Winrar etc), freeware and shareware.

- ITSS staff may automatically download and install software and upgrades, fixes and ‘plug-ins’ for software used by the College to improve the College IT facilities. If you require upgrades to College licensed software, please bring it to the attention of ITSS.

- Users should not deliberately or recklessly introduce or propagate any virus, worm, trojan horse, trapdoor or other harmful or nuisance program or file into the College IT network.

- Users should not attempt to install or use any software or hardware designed to record or transmit camera, sound, or control input on a machine without prior written authorisation from the Senior Leadership Team. Authorised recording or logging and storage of data gained must comply with applicable legislation and College policy.

- Users should not interfere with in any manner, or perform an unauthorised access of, the College's, any other company's or any person's hardware, software, or data.

- It is forbidden to attempt to set up servers or services on the network without written permission from the ITSS Manager.

2.16 Physical security of equipment

- All rooms containing IT equipment should be kept locked when not in use.

- Workstation related equipment should not be moved to another location (external) of the current recorded location for the hardware. A request for such a move should be made to ITSS in advance.

- Students should be instructed to vacate the location until the next member of staff arrives. The room should then be relocked.

- Any missing equipment should be reported to ITSS (ext. 411) immediately.

- Under no circumstances should students or non-ITSS staff be allowed access to the internal workings of any IT equipment.

- Where possible, computers should be fitted with physical security to prevent access and secured to room fittings to prevent removal from the recorded location.

- Staff and students should be encouraged to challenge any person carrying IT equipment off campus.

- Staff members with mobile apparatus are responsible for the safe transportation and storage of their College supplied equipment.

- Mobile devices such as laptops, tablets and smartphones should never be left unattended on display in vehicles in any location at any time.

- Staff/students seen to be vandalising/misusing IT equipment should be challenged (if deemed safe to do so) and reported to the IT Helpdesk.

- Any keys lost or misplaced for IT locations must be reported immediately to the Estates team.

2.17 Secure Disposal or Re-use of Equipment

- The College will ensure that where equipment is being disposed of all data on the equipment (e.g., on hard disks) is erased or physically destroyed.

- The College will ensure that where electronic media are to be removed from the premises for repair, where possible, the data is securely overwritten.

- A record of an asset's disposal will be maintained by the College.

- Disposal will be through a partner that fully complies with the government's current Waste Electric and Electronic Equipment (WEEE) Regulations to minimise environmental impact.

- All College owned IT equipment is the responsibility of the ITSS team, regardless of original budget holder, and should be returned to ITSS for reallocation at the end of a staff member's employment.

- All passcodes/passwords should be removed from devices upon their return so a factory reset can be successfully applied.

2.18 Security Monitoring

- The IT Systems & Services team is responsible for ensuring that the network is monitored for potential security breaches. All monitoring will comply with current legislation.

- Data of a personal nature should not be stored on College systems. This does not preclude access or removal of such a folder on the authority of the IT Systems & Services Manager.

At the discretion of the IT Systems and Services Manager, in consultation with the Strategic Leadership Team:

- The IT Systems & Services team reserves the right to access, modify or delete all data stored on or transmitted across the network. This includes data stored in personal network folders, mailboxes etc.

- The IT Systems & Services team reserves the right to disconnect or block any device connected either by physical or wireless means to the network.

- The IT Systems & Services team reserves the right to block any physical non-approved device connected to a piece of College owned equipment.

2.19 Reporting Data Security Breaches and Weaknesses

- Data security breaches and weaknesses, such as the loss of data or the theft of a laptop, must be reported in accordance with the requirements of the College's incident reporting procedure (appendix A) and, where necessary, investigated by the IT Systems & Services Manager.

2.20 Training and Awareness

- All users of the network must be made aware of the contents and implications of the IT and Data Security Policy.

- An Acceptable Use Policy summarising key points of this document must be accepted when logging onto domain joined Windows devices.

2.21 Disaster Recovery Plans

- The College will ensure that disaster recovery plans are produced for the network and that these are tested on a regular basis.

2.22 IT Systems & Services Team Responsibilities

The ITSS team will:

- Act as a central point of contact on network security within the College, for both staff and external organisations.

- Produce standards, procedures, and guidance on IT security matters for approval by the College.

- Co-ordinate network security activities particularly those related to shared information systems or IT infrastructures.

- Liaise with external organisations on network security matters, including representing the College on cross-community committees.

- Create, maintain, and give guidance on and oversee the implementation of network security.

- Represent the College on internal and external committees that relate to network security.

- Ensure that risks to IT systems are reduced to an acceptable level by applying security countermeasures identified following an assessment of the risk.

- Ensure that access to the College's network is limited to those who have the necessary authority and clearance. A log of privileged user accounts will be maintained.

- Support incident assessments, where necessary

- Ensure the security of the network, (that is information, hardware and software used by staff and, where appropriate, by third parties) is consistent with legal and management requirements and obligations.

- Ensure data is backed up on central systems.

- Ensure the physical security of central systems and networks, in collaboration with the Estates Team.

The responsibilities of our IT systems administrators include:

- Installing and maintaining device operating systems and network connections to reduce the chance of unauthorised access.

- Ensuring that system security patches are kept up to date where possible and such that the service is not adversely affected.

- Using privileged accounts only for systems administrative work and monitoring, not day-to-day activities.

- Ensuring that all software is properly licensed.

- Ensuring that knowledge of the super-user credentials is restricted.

- Administrators must not amend any audit or system information which may be used as part of an audit trail in cases of security breach.

- If necessary, to protect or maintain service, administrators will disconnect a system, individual workstation, or software from the College network.

- Monitoring activity and/or recording traffic on the network where appropriate, including periodic intrusion detection testing either internally or by third party.

- Maintaining central checking of malicious code, including of email passing through central mail systems.

2.23 User Responsibilities

Users of the network are responsible for:

- Safeguarding hardware, software, and information in their care.
- Preventing the introduction of malicious software on the College's IT systems.
- Reporting any suspected or actual breaches in security.
- Taking reasonable steps to ensure security of College machines, or on private computers which they attached to the College network either directly or over a VPN connection.
- Ensuring any personal device connected to the college network has the latest security updates applied and has an up-to-date anti-malware agent running.
- Notifying the IT Systems & Services team of security problems that may arise on their personal systems, and responding in a timely manner to security alerts put out by IT.

2.24 Contacts

In the event of an actual or suspected security incident, in the first instant, the user should contact the IT Helpdesk (01904 770411). The IT Helpdesk will then give instructions on how to proceed.

3 Data Security

3.1 Scope

Whilst working at York College, staff may have access to confidential or protected data. Data in electronic folders, on media, in documents, databases, spreadsheets, electronic mail, and any other format is considered within the scope of this section.

All **information and data** stored on York College systems whether networked, stand-alone or on associated computer storage media, are the exclusive and confidential property of York College. This data cannot be copied or disclosed to any other source, by any means, unless directed in writing by a Strategic Leadership Team member.

3.2 Handling Protected Information

During their work or studies, staff, and students (particularly research students) may handle information that comes under the General Data Protection Regulation (GDPR) or is sensitive or confidential in some other way. 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. If your role is likely to involve handling protected information, you must make yourself familiar with and abide by the GDPR guidance.

Remote Access

- 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.

Copyright information

- Almost all published works are protected by copyright. If you are going to use material (images, text, music, software), the onus is on you to ensure that you use it within copyright law. 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.

Others' information

- You must not attempt to access, delete, modify, or disclose restricted information belonging to other people without their permission, unless it is obvious that they intend others to do this, or you have approval from the IT Systems & Services Manager.

- Where information has been produced in the course of employment by York College, and the person who created or manages it is unavailable, the responsible line manager may give permission for it to be retrieved for work purposes. In doing so, 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 very specific circumstances governed by College and/or legal processes.

Publishing information

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

Representing the College - You must not make statements that purport to represent York College without the approval of the Director of Marketing.

Publishing for others - You must not publish information on behalf of third parties using the College's IT facilities without the approval of the Director of Marketing.

3.3 External Storage and Transfer of Data

- Where data is passed to third parties a formal agreement must be established and documented.

- The College Strategic Leadership Team (SLT) must approve formal agreements for the exchange of data and software between organisations.

- College data of any kind must not be stored on or transferred via any unauthorised external facility or cloud storage. This includes, but is not limited to Google Drive, Dropbox, and Apple iCloud.

- OneDrive/SharePoint/Teams are services which are provided as part of a College users account on Microsoft 365. These locations are authorised for storage and transfer of College Data (including Protected Data) provided that appropriate file security measures are in place (i.e., password protection and encryption.)

- Links sent to allow access to files and folders hosted in OneDrive should be of the time-limited variety and to specific users/groups rather than open access to anyone with the link. Such sharing should be revoked when it is no longer needed.

3.4 Removable Media

Removable media provide a common route for the introduction of malware and the accidental or deliberate export of sensitive data. In the normal course of business, it should not be necessary to use removable media, and the risk of doing so usually outweighs any perceived benefit.

Removable media is very easily lost, which can, and does, result in the compromise of large volumes of information. The loss of media can result in significant reputational damage, even if there is no evidence of what exactly has been lost. Removable media that is used to transfer information from one machine to another, for example a College PC to one at home, can be utilised by attackers to transport malicious software from one environment to the other.

This section is intended to outline responsibilities and controls around the use of removable media for its staff.

Removable media refers to any type of computer storage that is not physically fixed inside a computer. This includes, but is not limited to USB flash drives (aka USB sticks, USB pens, memory sticks), external hard disk drives, mobile devices used as external storage (e.g., smartphones, tablet local storage), and optical media (e.g., DVD, CD)

To ensure data is held securely, staff should refrain from transferring College data to removable media. Where data must be held on removeable media:

- Data in transit, whether sensitive or not, should only be stored on encrypted media. Data is assumed to be sensitive unless proven otherwise.

- Staff should not use un-encrypted removable media to store College data without prior approval. In such situations the data should be password protected, if possible.

- The user must maintain a log of what data is held on the device in case of loss/theft. This should not be kept on the same device.

- If the removeable media or any data is lost/stolen, it must be reported as soon as possible to the IT Systems & Services Manager or IT Team Leader, and the data log supplied.

- Data taken off premises should remain on the removeable media and not be copied to a third-party device unless prior approval has been given by the IT Systems & Services Manager or IT Team Leader.

- College provided removeable media and (where applicable) its password must not be shared with anybody else.

- Any passwords for encrypted media should not be written down.

- Staff should only store the minimum amount of data required to complete the business process on the removeable media.

- Staff should avoid using removable media for permanent or indefinite storage. Data should be transferred as soon as possible to a secure permanent store (either the College's file servers or Microsoft 365) and removed from the media when no longer needed.

- Sensitive data shall not be opened, read, or processed from public access computers.

- Before storing data on the provided/approved device consider whether a more secure alternative is available for access off campus i.e., viewing/sharing via College OneDrive/Teams/SharePoint in Microsoft 365, or by approved remote access solutions.

- Any removeable media devices issued to staff remain the property of the College and must be returned when staff leave the College's employment or no longer have a business use for such a device.

3.5 Cloud Services

Section 3.5 pertains to all external cloud services, e.g., cloud-based email, document storage, Software-as-a-Service (SaaS), Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), etc. Personal accounts are excluded.

It is imperative that staff do not open cloud services accounts or enter into cloud service contracts for the storage, manipulation or exchange of company-related communications or company-owned data without the IT Systems & Services Manager's input. This is necessary to protect the integrity and confidentiality of York College's data and the security of the corporate network.

The IT Systems & Services (ITSS) team remains committed to enabling staff to do their jobs as efficiently as possible through the use of technology. The following guidelines are intended to establish a process whereby the College's staff can use cloud services without jeopardising College data and computing resources.

If you are not sure whether a service is cloud-based or not, please contact the ITSS team.

- Use of cloud computing services for work purposes must be formally authorised by the IT Systems & Services Manager. The ITSS Manager will certify that security, privacy, and all other IT management requirements will be adequately addressed by the cloud computing vendor.

- For any cloud services that require users to agree to terms of service, such agreements must be reviewed by the IT Systems & Services Manager, with final approval from the Executive Director of Finance.

- Staff must not share log-in credentials for cloud services with colleagues or students. The ITSS team will keep a confidential document containing account information for business continuity purposes.

- The use of such services must comply with all laws and regulations governing the handling of personally identifiable information, corporate financial data or any other data owned or collected by York College.

- It is at the discretion of the IT Systems & Services Manager as to what data may or may not be stored in the Cloud.

- Personal cloud services accounts may not be used for the storage, manipulation or exchange of company-related communications or company-owned data.

    - College has selected Microsoft as its primary cloud storage provider for any College related data. Staff should not transfer any College data to any other third-party Cloud storage system without prior approval from the College's Data Protection Officer. This includes but is not limited to Dropbox, Google Drive, Box, iCloud, Mega, personal OneDrive.

- Staff should not store any personal information on College provided cloud storage.

3.6 Data Logging

The College's IT infrastructure provides a number of services to the York College community and beyond. In the process of providing these services, a number of logs are generated. These have a number of purposes including recording access and attempted access, maintaining an audit trail, provision of debugging information for troubleshooting, etc.

Depending on the purpose of the logs, they need to be retained for a period of time. There is an external expectation of being able to identify usage and attempted usage of systems for a reasonable period of time after the event. However, where logged information relates to the activities of living individuals, there is a competing requirement to not retain the information any longer than necessary.

This section describes how the IT Systems & Services team shall manage logs on systems for which it is responsible.

- Systems logs providing an auditable record of activity and attempted activity shall be retained for a minimum period of 3 months. This includes operating system logs, application software logs and usage reports, network traffic logs and exception files produced during network and email use.

- Access to logs shall be restricted to the custodian of the system and any other individuals with a legitimate need to access them.

- Logs shall be securely removed when no longer required.

- Logs shall be reviewed at an appropriate period to identify unauthorised and unusual activity patterns. Where logs are voluminous it may be appropriate for the review to be done using automated software tools.

- Systems shall be appropriately sized to ensure that they have adequate capacity to accurately collect and retain logging information.

- Logs shall be appropriately backed-up and/or copied into a central log repository in a timely fashion. This applies particularly to client systems that are regularly re-installed.

- Log files stored on the central log repository shall not be able to be changed by the administrators of the systems which generate the logs.

3.7 Data Backup and Restoration

- The IT Systems & Services team is responsible for ensuring that backup copies of data stored on the network are taken regularly.

- A log should be maintained of data backups detailing the date of backup and whether the backup was successful.

- Documented procedures for the backup process will be produced and communicated to all relevant staff.

- Users are responsible for ensuring that their own data is saved to Microsoft 365 cloud storage or network storage, and not local device storage.

- Patches and any fixes will only be applied by IT Systems & Services team following a suitable change control procedure.

4 Appendices

4.1 Appendix A - Incident Reporting Procedures

1. Introduction

The College and its employees, contractors and representatives use protected, sensitive, or confidential information (hereafter ‘protected data’) to further its mission and achieve operational objectives. It is required both by law and good practice that this data is handled and stored in a secure way and that any breaches of this security are prevented, mitigated, and responded to in a timely and responsible way.

Use and protection of data is discussed in the IT and Data Security Policy. This appendix addresses steps which must be taken in the event of a breach of security to report and mitigate the breach, and to identify actions which could be taken to prevent future breaches.

2. Reporting an incident

Breaches of data security including unauthorised access to protected data as well as loss or removal of devices which do or may contain protected data must be reported to IT Systems & Services (ITSS) via the **IT Helpdesk +44 (0)1904 770 411 or Ext 411 from a College phone.**

Loss of College property must also be reported to the Finance department (**Ext 407**) who will notify the Police of any theft which has occurred.

Breaches of physical security of the building or College fleet vehicles that may compromise data security must also be reported to the Estates Department (**Ext 209**).

If the above departments are unavailable, or a breach occurs out of College hours, notification should be made directly to the duty principal or manager on duty (**07973 807112**).

3. Managing the response to an incident

IT Systems & Services staff

When notified of a breach of data security, front-line ITSS staff will:

1. Act to prevent any ongoing data loss. For example, resetting compromised passwords or disabling affected accounts; removing access to data; isolating compromised systems.
2. Notify the IT Systems & Services Manager or the duty principal.

IT Systems & Services Manager, Duty Principal

The manager notified of a breach will be responsible for coordinating actions to mitigate and contain the breach.

They will also determine the severity of the breach and decide whether it can be dealt with within normal operations or is required to be notified to the Data Protection Officer (DPO) for the College or to the Strategic Leadership Team (SLT).

In addition, they will begin to compile a report of the nature of the breach and to document any action taken in response to it. This report is to be used later when reviewing the incident and may be required to be submitted to College senior management or external bodies as determined by the DPO.

DPO, SLT

In the event of a serious breach, the DPO will determine whether the Police or the UK Information Commissioner must be informed. Individuals affected will be informed without due delay if the breach is likely to result in a high risk of adversely affecting their rights and freedoms.

They will also determine whether the Principal, other members of SLT or the Board of Governors are required to provide an overall College response at this stage. They will then coordinate that response.

4. Reviewing the incident and managing risks

Managers involved should meet to review the causes of and response to the incident. They must ensure that all appropriate steps have been taken in response and identify any changes in procedure or other recommendations which may help reduce the risk or impact of similar incidents in the future.

These outcomes will be recorded as part of the incident report and progressed for inclusion in College policy or as advice to personnel as appropriate.

At a minimum, this meeting should involve the IT Systems & Services Manager and the manager of the College department(s) directly involved.

4.2 Appendix B – Data Security Breach Notification

The GDPR and Reporting Data Security Breaches

1. Introduction

This section covers, in brief, the requirements under the General Data Protection Regulation (GDPR) for detecting and reporting breaches of personal data security.

The Information Commission's Office (ICO) is responsible for upholding information rights for UK persons and companies and is the body to whom breaches are reported.

Additional guidance is available from the ICO website:
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

In particular, the section handling breaches:
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/

The GDPR replaces the Data Protection Act (1998) and came fully into force on the 25th May 2018. While the regulation covers a full approach to managing and securing data, this appendix is intended only to provide guidance on the procedure to follow in the event of a breach (or suspected breach) of personal data.

As defined under the GDPR, the College acts as a 'Data Controller'. All persons or companies acting on or with personal data controlled by the College at its direction or on its behalf is acting as a 'Data Processor'.

Upholding the College's legal obligations under GDPR is a duty of all College employees, or anyone acting on behalf of the College, regardless of role. They should be familiar with the requirements of GDPR to fully meet the College's obligations. The College has been providing Data Protection and training to all staff and will continue to offer help and support.

Any person who becomes aware of, or suspects, a breach of data security is required to report it immediately even if handling this data is not normally a part of their role at the College. These persons should follow the procedures assigned to the data processor below.

2. Definition of a Data Security Breach

From the ICO guidance, a data breach is defined as:

"*…a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.*"

Both accidental and deliberate breaches are included as are breaches caused by inaction, and a breach is not just about loss of personal data.

Examples of breaches from a College perspective can include (but are not limited to):

- Access by an unauthorised third party, student, or member of staff.
- Sending personal data to an incorrect recipient, even if under other circumstances that recipient may be authorised to access and process that data.
- Loss or theft of any equipment containing personal data, not just College issued devices.
- Personal data being altered without permission.
- Loss of availability to personal data (for example, faulty or destroyed media).

Any incident which affects the confidentiality, integrity or availability of personal data is a data security breach and this procedure must then be followed.

3. Breach Reporting for Data Processors

Firstly, don't panic. A hasty action can expose data further so take a moment to consider what actions are immediately practical to close the breach without exacerbating it or exposing further data. This may include seeking advice from IT Systems & Services, for example to recall or stop an email sent in error or to remove file access from an unauthorised person.

Then, or if no action is immediately practical, contact the College's Data Protection Officer (DPO) to inform them of the breach. If they are not available, contact whichever senior manager is currently the Duty Principal via College Reception on 01904 770200. After you have reported the breach you will need to record all details known to you about the breach and any steps you took to close it before you contacted the DPO. You will need to hand this document to the DPO and then co-operate with their investigation.

It is the responsibility of the DPO to record the breach fully and decide whether it must be reported to the ICO, however you should continue to record and notify the DPO of any further actions you take or information you become aware of regarding the breach. You should retain a copy of your record in case it is required later.

4. Role of the Data Protection Officer

It is the duty of the Data Protection Officer for the College to:

- fully record all data security incidents and ensure retention of these records whether they are reported to the ICO or not.
- supervise planning and implementation of actions to close the breach, secure affected data or mitigate the loss.
- decide whether the breach must be notified to the ICO and carry out such notification. This must be done within 72 hours of the breach.

- prompt and inform any necessary review of College processes to reduce the likelihood or impact of future similar breaches.
- present their report on the incident to senior management and / or the governing body as appropriate.

5. ICO Breach Notification

Notification of data security breaches should be carried out by the College DPO and follow the current process appropriate to the type of incident as outlined on the ICO website:

https://ico.org.uk/for-organisations/report-a-breach/