Policy / Procedure Title: IT SECURITY POLICY 2018
Developed By: Azhar Iqbal, IT and Systems and Services Manager
Date Developed:
Date Of SMT Approval:
Date of Impact Assessment:

Date Of Next Review: April 2020

Please contact us on 01904 770132 or email us at mramsden@yorkcollege.ac.uk if you would like this document in an alternative format

Please contact Azhar Iqbal on 01904 770423 or email aiqbal@yorkcollege.ac.uk if you have any questions about all or part of this document.

York College IT Security Policy

Contents

1.0 Introduction

1.1 York College has developed an IT Security Policy to achieve the following key points:

- Availability (knowing that the information can always be accessed by the relevant authorised users);
- Integrity (knowing that the information is accurate and up-to-date, and has not been deliberately or inadvertently modified from a previously approved version);
- Confidentiality (knowing that sensitive information can be accessed only by those authorised to do so).

1.2 Need for a Security Policy

The data stored in manual and electronic systems used by York College represent an extremely valuable asset. The increasing reliance on information technology for the delivery of college service makes it necessary to ensure that these systems are developed, operated, used and maintained in a safe and secure fashion in addition to paper based records.

The increasing need to transmit information across networks of computers renders the data more vulnerable to accidental or deliberate unauthorised modification or disclosure.

1.3 Legal Requirements

Some aspects of information security are governed by legislation, the most notable U.K. Acts are:

- The Data Protection Act (2018)
- General Data Protection Regulation (2018)
- Copyright, Designs and Patents Act (1988)
- Computer Misuse Act (1990)
- Regulation of Investigatory Powers Act (2000)
- Freedom of Information Act (2000)
- Human Rights Act (2000)
- PREVENT Strategy (2011)

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.

1.4 Terms

The following terms are used in this document:

Users – Any persons using College IT equipment or infrastructure, or who has access to College-held data.

Data – Any information held by the College on its IT systems or devices.

Protected data – Any data held by the College which is defined as 'Personal' or 'Protected' under the Data Protection Act (1998) or GDPR (2018).

Device(s) – Any Equipment owned by the College or used to access College infrastructure or data.

1.5 Who is affected by the Policy?

The Policy applies to all employees and students of the college. It also applies to contractors and visitors, not employed by the college but engaged to work with or who have access to College IT equipment, infrastructure or data.

The policy applies to all use of College IT equipment whether on site or off-site including use of third party data connections.

The policy applies to all use of the College's IT infrastructure and data regardless of the device or method used to connect.

1.6 Where the Policy Applies

The Policy applies to all locations from which college systems are accessed, or College equipment or data is used, including home use or other remote use.

Where there are links to enable non-college organisations or users to have access to college data or systems, the college must confirm the security policies they operate meet our security requirements or the risk is understood and mitigated. The Policy applies to all systems and all data whether academic, administrative or any other.

1.7 Responsibilities

1.7.1 IT Systems and Services (ITSS) is responsible for:

- ensuring the security of central information systems and the college IT network;
- backing up data on central systems;
- providing advice and guidance on information security;
- ensuring the physical security of central systems and networks, in collaboration with the Estates Team.

1.7.2 College Departments are responsible for:

- ensuring the security of departmental information systems, and networks where applicable;
- registering with ITSS equipment attached to the college network for which the department is responsible;
- notifying ITSS of security problems that may arise on departmental systems
- encouraging good information security practice among staff and students
- ensuring the physical security of departmental systems in collaboration with the Estates Team.

1.7.3 Individual users of college information systems are responsible for:

- taking reasonable steps to ensure security on their College machines, or on private computers which they attached to the college network either directly or over a dial-up/VPN connection;
- registering with ITSS equipment attached to the college network for which they are personally responsible;
- backing up data on their College or private machines;
- notifying ITSS of security problems that may arise on their personal systems, and responding in a timely manner to security alerts put out by ITSS;
- taking reasonable steps to ensure there is no unauthorised access to systems they are responsible for;
- preserving the confidentiality of passwords;

1.8 Contacts

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

2.0 IT Resource and Internet Usage Policy

2.1 Internet access and IT facilities are provided by York College for use in the furtherance of the College's mission. York College aims to provide you with accessible, up-to-date and reliable Information and Learning Technology to support you in your work, research and studies.

2.2 To help ensure that we maintain this level of provision the College has established this Policy regarding all uses of College IT resources and access to the Internet via the College's IT Network.

2.3 The college intends to enforce this policy, but reserves the right to change it at any time as circumstances may require. The IT Systems and Services Manager (ITSS) Manager is responsible for administering this policy and should be contacted should you have any questions or comments concerning this policy.

2.4 This Policy applies to any use of College IT resources or use of the Internet when using the College IT Network.

2.5 Use of College IT facilities and access to the Internet, including College cloud services such as email may be suspended at the College's discretion if a breach of this policy is detected or suspected to prevent further incident or to enable investigation. Use may also be suspended for staff or students who are subject to disciplinary proceedings in accordance with this or other College policies.

2.6 In using the Internet via College systems, users shall not:

a) Make unreasonable use of personal internet service e-mail accounts. i.e. excessive use during working hours or during lessons.

b) Participate in on-line:
   (i) gambling;
   (ii) non-educational games; or
   (iii) non-academic social media.

c) Access, download, create, transmit or store:
   (i) any illegal, offensive, obscene or indecent images, data or other material, or any data that may be resolved into obscene or indecent images or material;
   (ii) any material which is designed or likely to cause annoyance, offence, inconvenience or needless anxiety;
   (iii) any defamatory or libellous material;

(iv) any material that infringes the copyright of another person/organisation;
(v) any unsolicited commercial or advertising material; or
(vi) any other material which may expose the College to legal liability.

d) Use the College's IT network to download or distribute pirated, 'cracked' or otherwise illegal or infringing versions of licensed software or data.

e) Install any software on the hard disk of a computer or the college network without first obtaining permission to do so from the ITSS 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.

f) Download software and upgrades, fixes and 'plug-ins' for any software. The exception to this is staff in ITSS, who may download software and upgrades, fixes and 'plug-ins' for software used by the college in order to improve the college IT facilities. If you require upgrades of this type to college licensed software, please bring it to the attention of ITSS.

g) Copy, or attempt to copy, any college licensed software for private use.

h) Deliberately introduce or propagate any virus, worm, Trojan Horse, trap-door or other harmful or nuisance program or file into the college IT network.

i) 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 Management Team. Authorised recording or logging and storage of data gained must comply with applicable legislation and College policy.

j) Access, download, transmit or store information or materials owned by another party that are protected by copyright, trade secret or other intellectual property rights without the proper consent of the owner of such rights. Copyright applies to all text, pictures, video and sound.

k) Harass, demean or defame any person, including, without limitation, sexually harassing, discriminating against or defaming any person based upon that person's race, gender, disability, sexual orientation, age, ethnicity or religious beliefs, gender identity, marriage/civil partnership, pregnancy/maternity/paternity.

l) Access or transmit any confidential, proprietary or trade secret information of the college including, without limitation, information concerning the college's finances and business operations without prior written consent of a member of the Senior Management Team.

m) Express any political or religious information, views or opinion in contravention of the college's Equal Opportunities Equality & Diversity policy.

n) Broadcast any information to bulletin boards or public newsgroups or persons that are not directly associated with the college.

o) Become a member or associate with any non-work related chat group, newsgroup or audio conference facility etc.

p) Conduct, or solicit or use the College IT Networks for work you perform outside work/studies associated with the College (for example, but not limited to, political causes, personal, religious, charitable or other commercial ventures) without prior written agreement from a member of SMT.

q) 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.

r) Use the college internet facilities to disable or overload any computer system or network, or to circumvent any system intended to protect the privacy or security of others.

s) Enter the College, its staff or students into any financial obligations through the use of the internet. The exception to this is purchases on behalf of the College made in accordance with the College's financial regulations.

t) Use the College communications network to sign up with websites or organizations that offer rewards, monetary or otherwise, for surfing the internet.

u) For reasons of security, make their password known to anyone else.

2.7 The above list of prohibited actions is by way of example only and is not intended to be exhaustive. In any access or use of the Internet, staff and students are expected to act in a professional, business like and ethical manner and remember at all times that you are a representative of the College.

2.8 At any time, the College at its sole discretion, can access, restrict access to, modify or remove, either permanently or temporarily, any information that has been downloaded using the IT Network and equipment of the college.

2.9 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.

2.10 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;
- On-line gambling;
- On-line games or computer game related;
- Hatred or intolerance;
- Violence;
- Incitement to extremism;
- Threats to the security of the service or stored data.

2.11 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.

2.12 If a student or staff member needs access to a resource which is blocked due to this **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, or via a user's line manager or class/progress tutor. Each case will be reviewed independently based on the reasons provided by the requesting party.

2.13 Access to the Internet from College devices shall be via the College IT Network. Personal connection to the internet via third party services is strictly forbidden, except where prior written approval has been obtained from either the ITSS Manager or a member of the senior management team.

2.14 The use of IT resources and the Internet by staff must strictly conform to this Policy and must not hinder or interfere in any manner with the duties of their job and responsibilities to the college. Any violation of this policy may result in disciplinary action, including, in appropriate circumstances, dismissal.

2.15 The use of IT resources and the Internet by students must strictly conform to this Policy and must not hinder their studies or those of other students.

Any violation of this policy may result in disciplinary action, including, in appropriate circumstances, exclusion.

2.16 The use of IT resources and the Internet by contractors or visitors to the College must strictly conform to this Policy and be in accordance with the conditions under which they were granted access. Any violation of this policy may result in access being revoked and a complaint being lodged with the represented company/organisation.

2.17 Any violation of this policy may also be subject to penalties under criminal or civil law (for example, but not limited to, Data Protection Act 1998, Copyright, Designs & Patents Act 1988, Computer Misuse Act 1990) and such law may be invoked by the College, or violations reported to the appropriate body, or to the police.

2.18 Use of College IT services including Internet and email usage may be grounds for referral under the PREVENT strategy, may be submitted as part of a referral, or requested by investigating parties.

2.19 Members of staff, students, contractors or visitors may not access the Internet via the college's IT Network at any time, through any device, unless they have read and understood this policy. By using the college's IT resources users confirm they understand and agree to be bound by this policy.

3.0 Email Usage Policy

3.1 Users of college email facilities should be aware of the following:

3.1.1 Email facilities provided by York College for use by college employees and students are for the furtherance of the college's mission. 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.

3.1.2 All users of college email facilities will be periodically notified of this policy via email as well as by continuous posting on the Intranet.

3.1.3 Inappropriate use of email facilities may lead to disciplinary action.

3.1.4 Use of email facilities may be suspended for staff or students who are subject to disciplinary action.

3.1.5 Incidental personal use of email is permitted but must always remain within the parameters stated in this policy.

3.1.6 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.

3.1.7 All email messages leaving the college should be **legal, decent, honest and appropriate to their recipient.**

3.1.8 Users are prohibited from using the college network to:

a) 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.
b) Spread gossip, rumours, or innuendos about employees, learners, clients, suppliers, or other outside parties.

c) Send, receive, solicit, print, copy, or reply to sexually oriented messages or images.
d) Send, receive, solicit, print, copy, or reply to messages or images that contain foul, obscene, or adult-oriented language.
e) Send, receive, solicit, print, copy, or reply to messages or images that are intended to alarm others, embarrass the college, negatively impact employee/learner productivity, or harm employee/learner morale.

3.1.9 Messages should not:

Slander, defame, infringe employee 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.

3.1.10 College employees 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.

3.1.11 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.

For further information, please visit http://its.yorkcollege.ac.uk/EmailUsagePolicy

---

3.1.12 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.

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

3.1.14 In order to prevent the system from slowing down as a result of the space taken by large attached files (such as games, screensavers and pictures) and subsequently circulated, attachments of this kind must not be circulated within the college. They must be forwarded to the ITSS Team where they will be checked and if appropriate, placed on the college's Network from where they may be downloaded. Once the attachment has been forwarded, users must delete it immediately from their inbox and from sent mail.

3.1.15 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.

3.2 Privacy

3.2.1 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 any particular message or that any message was actually sent or received.

3.2.2 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.

3.2.3 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 SMT, email access may be delegated to an employee's line manager.

3.2.4 When an employee 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.

3.2.5 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. Employees have no reasonable expectation of privacy when it comes to business and personal use of the college's email system.

3.2.6 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 any and all usage of email, and any and all files, information, software, and other content created, sent, received, downloaded, uploaded, accessed, or stored in connection with

employee 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 employee / student. This includes referrals or investigatory requests made under the PREVENT strategy.

3.3 College Notices

3.3.1 Relevancy to College business

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

3.3.2 Staff leaving party / collections

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

3.3.3 Personal announcements

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

3.3.4 Student Notice distribution

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 intranet site, workstation notice screens, digital signage, etc).

Messages only for students on particular courses or in particular divisions can be sent using the appropriate group in the email address book. 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.

3.3.5 Spelling, Grammar, Wording

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.

3.3.6 **Attachments and embedded images**

These 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.

3.3.7 **Formatting**

College communications policy requires that text for publication be set out in a 12pt Arial font. Notices which differ from this to the point of potentially causing difficulty to readers will be returned to the sender for reformatting.

3.3.8 **Content**

Guidelines set out elsewhere in the College Email Usage Policy relation to content of messages also apply to College Notices. 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 back to the originator for clarification or rewording.

4.0 Communications and Infrastructure Usage Policy

4.1 Wired LAN Security

4.1.1 **Purpose**

The purpose of this policy is to address the security vulnerabilities and responsibilities associated with the wired LAN (Local Area Network) within York College, and to establish appropriate procedures to ensure the protection of the existing data communications infrastructure.

4.1.2 Goals

The goals of this policy are to:

- Limit the potential security risks that are associated with computer networks, by ensuring that only authorised users are allowed access to the College networks.
- Ensure the confidentiality, integrity and authenticity of data as it transverses the college's network.
- Identify and patch possible security holes that could compromise the college's network.
- Ensure that the college's network remains secure, by monitoring the state of security arrangements.
- Ensure the effectiveness of this policy, by means of security testing to identify weaknesses.
- Improve and update network security in response to monitoring, testing and new risks.

4.1.3 Requirements

- All network devices that constitute part of the York College campus network shall be of a make and design identified, approved, and deployed by ITSS.
- 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 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.

4.2 Wireless LAN Security

4.2.1 Purpose

The purpose of this policy is to address the security vulnerabilities and responsibilities associated with wireless networking on the York College campus, and to establish appropriate procedures to ensure the protection of the existing data communications infrastructure.

4.2.2 **Goals**

The goals of this policy are to:

- Limit the potential security risks that may be associated with wireless network technologies; i.e. by ensuring that only authorised users are allowed to access the network.

- Educate the College IT Users about the security concerns associated with wireless networks.

- Establish campus wide policies for the deployment of wireless networks.

4.2.3 **Requirements**

ITSS shall administer the wireless LAN network within the York College campus and will provide access points (APs) supporting IP

(Internet Protocol) connectivity to the data communications network at various locations throughout the college's Campus.

- 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.

- 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. Communications and Infrastructure support 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 ITSS.

- Any attempt to physically alter or remove APs by any user other than ITSS is strictly prohibited.

4.3 Remote Access Policy

4.3.1 Purpose

The purpose of this policy is to address the security vulnerabilities and responsibilities associated with remote access to the York College network. These standards are designed to minimize the damage that may result from the unauthorised access to York College resources via remote access. Damage includes the loss of sensitive or company confidential data, intellectual property, damage to public image; damage to critical College systems, etc. Remote access implementations that are covered by this policy include, but are not limited to, dial-in modems, ISDN, DSL, VPN, and cable modems, etc.

4.3.2 Goals

It is the responsibility of college employees, 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.

The goals of this policy are to:

- Limit the potential security risks that may be associated with wireless network technologies; i.e. by ensuring that only authorised users are allowed remote access to the network.
- Educate the campus communities about the security concerns associated with remote access.
- Establish campus wide policies for the use of remote access to the college network.

4.3.3 Requirements

- Secure remote access must be strictly controlled. Control will be enforced via the Colleges VPN gateway.
- At no time should any college employee provide their login or email password to anyone, not even family members.
- All hosts that are connected to York College internal networks via remote access technologies must use the most up-to-date anti-virus software, this includes personal computers.

- Personal equipment that is used to connect to York College owned networks must meet all the requirements of York College equipment for remote access.

4.4 Virtual Private Network (VPN) Policy

4.4.1 Purpose

The purpose of this policy is to provide guidelines for Remote Access using Virtual Private Network (VPN) connections to the York College corporate network.

4.4.2 Goals

Approved York College employees, and authorised third parties (customers, vendors, etc.) may utilize the benefits of VPN's, which are a "user managed" service. This means that the user is responsible for selecting an Internet Service Provider (ISP), coordinating installation, installing any required software, and paying associated fees.

The goals of this policy are to:

- Limit the potential security risks that may be associated with VPN technologies; i.e. by ensuring that only authorised users are allowed VPN access to the network.

- Educate the campus communities about the security concerns associated with VPN access.

- Establish campus wide policies for the use of VPN access to the college network.

4.4.3 Requirements

- It is the responsibility of employees with VPN privileges to ensure that unauthorised users are not allowed access to York College internal networks.

- VPN gateways will be set up and managed by York College network operational groups.

- All computers connected to York College internal networks via VPN or any other technology must use the most up-to-date anti-virus software.

- VPN users will be automatically disconnected from York College's network after thirty minutes of inactivity. The user must then logon again to reconnect to the network.

- The VPN concentrator is limited to an absolute connection time of 24 hours.

- Users of computers that are not York College-owned equipment must configure the equipment to comply with York College's VPN and Network policies.

- Only college approved VPN clients may be used.

- By using VPN technology with personal equipment, users must understand that their machines are a de facto extension of York College's network, and as such are subject to the same rules and regulations that apply to York College-owned equipment, i.e., their machines must be configured to comply with Network security administrator/team Security Policies.

4.5 Telephone Usage Policy

Voice and other communications which occur over College telephony devices are monitored for a variety of reasons. Monitoring actions for physical or soft phones are detailed her. Users of College issued mobile phones should refer to the separate Mobile Usage Policy. Use of personal mobile devices is covered in the Internet usage and WiFi network usage sections of this document.

Communications via desk phones and computer based soft phone using the College's telephony infrastructure is logged and monitored for legal, system integrity and cost reasons, and may be referred to for 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 held in these logs will be held securely and made available only in accordance with College policies.

5 Passwords and Data Security

5.1 Data and File storage/security

5.1.1 Whilst working at York College, staff may have access to confidential or protected data. This data cannot be copied or disclosed to any other source by any means unless directed in writing by a senior member of staff (SMT). Data in electronic folders, on media, in documents, databases, spreadsheets, electronic mail, and any other format is considered within the scope of this policy.

- All **information and data** stored on York College Information systems, and associated computer storage media are the exclusive and confidential property of York College. Use or conveyance of this data to unauthorised personnel may result in immediate disciplinary action which may lead to employment termination.

- All **information and data** stored on other York College systems, both networked and stand-alone are the exclusive and confidential property of York College and the individuals being supported. Use or conveyance of this data to unauthorised personnel may result in immediate disciplinary action which may lead to employment termination.

5.1.2 Users must not gain access or attempt to gain access to any files owned by someone else unless the owner has specifically granted access.

5.1.3 Users must not use equipment in contravention of the law.

5.1.4 Users must not install software on shared equipment without the authorisation of the ITSS Manager.

5.2 External Storage and Transfer of Data

5.1.5 **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.

5.2.1 The OneDrive facility which is provided as part of staff accounts on Microsoft Office 365 is 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.)

5.2.2 Links sent to allow access to files and folders hosted in OneDrive should be of the time-limited type and such sharing should be revoked when it is no longer needed.

5.2.3 Portable storage devices (e.g. USB drives, portable hard drives, optical disks, etc.) should not be used to store or transfer Protected or Sensitive Data.

5.3 User ID/Password

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

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

5.3.3 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.

5.3.4 Accounts should not be re-used, except where absolutely necessary, and under the condition that details are kept of the users of the account.

5.3.5 Lists of users and their data (such as usernames) must not be available to anonymous users or, where possible, to other users and systems administrators.

5.3.6 Computers in open areas should be physically secured.

5.3.7 Authorised users are allocated a username and password, and must ensure that nobody else uses it. The user is responsible for the confidentiality of the username and password.

5.3.8 Users must not use anyone else’s username/password.

5.3.9 Users must not obtain or try to obtain anyone else’s password.

5.3.10 Users must inform ITSS immediately if they suspect someone else of using their username/password.

5.3.11 Office computers must not be left unattended when logged in. If you need to leave the PC, lock the computer via CTR-ALT-DEL Lock workstation.

5.3.12 Shared computers must not be left unattended when logged in.

5.4 Systems Administrators

The responsibilities of system administrators should include:

5.4.1 Install and maintain the operating system and network connection in order to reduce the chance of unauthorised access.

5.4.2 Ensure that systems security patches are kept up to date where possible and such that the service is not adversely affected.

5.4.3 Users including systems administrators, should normally login with userids without unnecessary (“super-user”) privileges. Privileged accounts should be used only for systems administrative work and monitoring.

5.4.4 When undertaking systems work demanding privileged user status, administrators should login in under their own account before assuming privileged status (to maintain audit information).

5.4.5 Administrators must ensure that all software is properly licensed.

5.4.6 Ensure that passwords are changed regularly and knowledge of the super-user password should be restricted.

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

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

5.4.9 Monitor activity and/or record traffic on the network if appropriate, including periodic intrusion detection testing either internally or by third party.

5.4.10 Maintain central checking of malicious code, including of email passing through central mail systems.

6.0 Physical Security of IT Equipment

6.1 Security of IT Related Equipment.

The following section is directed at the secure and safe handling of ITSS related equipment, both location fixed and mobile.

6.2 ITSS Equipment Security Policy.

6.2.1 All rooms should be kept locked at all times when not in use.

6.2.2 All workstation related equipment should not be moved to another location (external) of the current recorded location for the hardware. ITSS to be informed of any such movements in advance.

6.2.3 When in teaching rooms, students should never be left unattended for any reason.

6.2.4 Access to student rooms should only be granted by the member of staff next using the location.

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

6.2.6 Any missing equipment should be reported to ITSS (ex 411) immediately.

6.2.7 Any suspicious behaviour should be reported to Estates on ext 209 immediately.

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

6.2.9 Where possible, base units should be fitted with physical security to prevent access, and also secured to room fittings to prevent removal from the recorded location.

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

6.2.11 All staff should be carrying and displaying their ID badge at all times.

6.2.12 Staff members with mobile apparatus are responsible for the safe transportation and storage of their own college supplied equipment.

6.2.13 Mobile equipment should never be left unattended at any time unless other staff members are present or the location can be locked, (excluding vehicles).

6.2.14 PDA, Blackberry and laptops should never be left unattended on display in vehicles in any location at any time.

6.2.15 Staff / Students seen to be vandalising / miss using IT equipment should be challenged (if deemed safe to do so) and reported to ex. 209 immediately.

6.2.16 Use of any IT equipment is covered by the acceptable Usage Policy, this policy can be revised at any time by management.

6.2.17 Any keys lost or misplaced for IT locations must be reported immediately to Estates on ex. 209.

7.0 Appendices

7.1 Appendix A - Best Practice and Guidance

York College IT Security Policy covers a wide range of subjects with regards to IT security, and some of the topics can be a little overwhelming. However, it is important that we all understand the key aspects of the policy to ensure that we adhere to legislation as well as keeping our data secure.

The following points are quick best practice pointers that should be read alongside the policy itself.

1. Use of memory sticks

Flash memory devices (such USB memory sticks) and external storage devices provide a very useful function in that they can hold large amounts of data in a small portable device. However, the very nature of their use can also provide a security problem. The College regularly has these devices handed in to lost property, and it is sometimes alarming to see what is stored on to these devices. Under the Data Protection Act, the College needs to ensure that it safe guards all its data, and this includes what may be stored on a memory stick. **Those staff who use memory sticks as part of their work should ensure that these devices are password protected and that they do not contain any personal or sensitive data. If they are to hold other important data, then an added level of security must be used - and we recommend that this added security should be encryption**. Some USB keys come with their own encryption software, however if none is present then free open source versions are available from various companies. This software can be used to encrypt a folder on a USB key, and the data in this folder can then be stored more securely. Most of these companies also provide step by step guides on their website that explains how to install and use this software.

2. Use of laptops/tablets

As with USB memory sticks, portable devices such as laptops and tablets can hold sensitive or protected data and as such users need to ensure that they keep data secure. Unless there is a business need, then all sensitive data should be stored on the network. If you do need to store sensitive data on your laptop/tablet, then ensure that you use security software such as the encryption software that was mentioned above to encrypt the folder that you store this data into.

When using your device on the network then you should also ensure that you observe best practice guidelines such as:

- Ensure your Antivirus is kept up to date - on managed PCs this is done centrally, however you should regularly check that the updates are occurring.
- When checking emails, do 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 the email without checking with the sender the reason/purpose of the link.

Additionally, users of laptops/tablets are responsible for the security of their devices, and should ensure that they are kept safe in terms of where they are stored or used. Never leave the device unattended in open view such as in a classroom, staffroom or even a car. If you do need to leave it in your car, then store it out of sight such as in the boot of the car.

3. Network account passwords

Ensure that your password is kept safe i.e. don't write it down or divulge it to anyone else. The College's network will force you to regularly change your password, and you should try to ensure that you use complex passwords i.e. use a mixture of letters, numbers and special characters.

7.1 Appendix B - Incident Management 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 Information 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 via the **IT Helpdesk +44 (0)904 770 411 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 assistant 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 ITS&S 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 manager or the assistant principal on duty.

IT Manager, Duty AP

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 for the College or to the Senior Management Team.

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, SMT

In the event of a serious breach, the DPO will determine whether the Police or the UK Information Commissioner must be informed.

They will also determine whether the Principal, other members of SMT 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 Manager and the manager of the College department(s) directly involved.

7.3 Appendix C – Data Security Breach Notification

The GDPR and Reporting Data Security Breaches (Draft – Jan 2018)

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 comes fully into force on the 25th May 2018. While the regulation covers a full approach to managing and securing data, this document 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 in order 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 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/

An example form for reporting a breach is published by the ICO. This is reproduced below and should be used as a reference to staff regarding what information may be required for a report.

ico.
Information Commissioner's Office

Data protection breach notification form

This form is to be used when data controllers wish to report a breach of the Data Protection Act to the ICO. It should not take more than 15 minutes to complete.

If you are unsure whether it is appropriate to report an incident, you should read the following guidance before completing the form: Notification of Data Security Breaches to the Information Commissioner's Office.

Please provide as much information as possible and ensure that all mandatory (*) fields are completed. If you don't know the answer, or you are waiting on completion

of an internal investigation, please tell us. In addition to completing the form below, we welcome other relevant supporting information, eg incident reports.

In the wake of a data protection breach, swift containment and recovery of the situation is vital. Every effort should be taken to minimise the potential impact on affected individuals, and details of the steps taken to achieve this should be included in this form.

1. Organisation details

(a) * What is the name of your organisation – is it the data controller in respect of this breach?

(b) Please provide the data controller's registration number. Search the online Data Protection Public Register.

(c) * Who should we contact if we require further details concerning the incident? (Name and job title, email address, contact telephone number and postal address)

2. Details of the data protection breach

(a) * Please describe the incident in as much detail as possible.

(b) * When did the incident happen?

(c) * How did the incident happen?

(d) If there has been a delay in reporting the incident to the ICO please explain your reasons for this.

(e) What measures did the organisation have in place to prevent an incident of this nature occurring?

(f) Please provide extracts of any policies and procedures considered relevant to this incident, and explain which of these were in existence at the time this incident occurred. Please provide the dates on which they were implemented.

3. Personal data placed at risk

(a) * What personal data has been placed at risk? Please specify if any financial or sensitive personal data has been affected and provide details of the extent.

(b) * How many individuals have been affected?

(c) * Are the affected individuals aware that the incident has occurred?

(d) * What are the potential consequences and adverse effects on those individuals?
(e) Have any affected individuals complained to the organisation about the incident?

4. Containment and recovery

(a) * Has the organisation taken any action to minimise/mitigate the effect on the affected individuals? If so, please provide details.

(b) * Has the data placed at risk now been recovered? If so, please provide details of how and when this occurred.

(c) What steps has your organisation taken to prevent a recurrence of this incident?

5. Training and guidance

(a) As the data controller, does the organisation provide its staff with training on the requirements of the Data Protection Act? If so, please provide any extracts relevant to this incident here.

(b) Please confirm if training is mandatory for all staff. Had the staff members involved in this incident received training and if so when?

(c) As the data controller, does the organisation provide any detailed guidance to staff on the handling of personal data in relation to the incident you are reporting? If so, please provide any extracts relevant to this incident here.

6. Previous contact with the ICO

(a) * Have you reported any previous incidents to the ICO in the last two years?

(b) If the answer to the above question is yes, please provide: brief details, the date on which the matter was reported and, where known, the ICO reference number.

7. Miscellaneous

(a) Have you notified any other (overseas) data protection authorities about this incident? If so, please provide details.

(b) Have you informed the Police about this incident? If so, please provide further details and specify the Force concerned.

(c) Have you informed any other regulatory bodies about this incident? If so, please provide details.

(d) Has there been any media coverage of the incident? If so, please provide details of this.

Sending this form

Send your completed form to casework@ico.org.uk, with 'DPA breach notification form' in the subject field, or by post to: The Information Commissioner's Office,

Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF. Please note that we cannot guarantee security of forms or any attachments sent by email.

What happens next?

When we receive this form, we will contact you within seven calendar days to provide:

- a case reference number; and
- information about our next steps

If you need any help in completing this form, please contact our helpline on **0303 123 1113** or **01625 545745** (operates 9am to 5pm Monday to Friday)