EDA COLLEGE

Information Security Policy

Version Control

Version	*1.1*
Approved by	*Academic Board*
Approval date	*Dec 2024*
Next review date	*Dec 2025*
Policy owner	*Principal*

Contents

Introduction

All information held by the EDA College, in all formats, represents an extremely asset and, therefore, must be used and stored in a secure manner.

This Policy is in two parts;

First Part outlines security procedures covering all aspects of processing information.

Second part covers security of IT systems.

The Policy must be read in conjunction with other Information and IT Policies, including:

- Data Protection Policy
- Information Security Policy
- ICT Policy
- Incident response Management Policy

The Policy applies to all staff member and students. It also applies to contractors, business partners and visitors, not employed by the college but engaged to work with or who have access to college information, (e.g. computer maintenance contractors) and in respect of any externally hosted computer systems.

The Policy applies to all locations from which college systems are accessed (including home use). A copy of any relevant third-party security policy should be obtained and retained with the contract or agreement.

EDA approach to Information Security

EDA College will:

- Use all reasonable, appropriate, practical and effective security measures to protect its e-processes and information assets from inappropriate use.
- Continually examine ways in which it can improve the use of security measures to protect and enhance its students and staff interests.
- Protect and manage its information assets in such a way as to comply with its contractual, legislative, privacy and ethical responsibilities.

Policy Compliance

Senior management should ensure all staff are aware of and understand the content of this policy.

If any user is found to have breached this policy, they could be subject to disciplinary and misconduct procedures as outlines in respective conduct policies and Dismissal Policy & Procedure. Serious breaches of this policy could be regarded as gross misconduct.

Legal Aspects

Some aspects of information security are governed by legislation, the most notable UK Acts and European legislation are listed below:

- The Data Protection Act (2018)

- General Data Protection Regulation (GDPR)
- Copyright, Designs and Patents Act (1988)
- Computer Misuse Act (1990)

Responsibilities

Responsibilities of the College in relation to Information

- Will respect the concept of academic and individual freedom but will expect its Information Users to ensure that colleagues and the College are not disadvantaged or penalised by inappropriate information security actions.
- Will charge the IT Manager with responsibility for developing and implementing this Information Security processes who will report on information security issues, monitor progress and recommend appropriate actions.

Senior Management

Senior Management must:

- be aware of information or portable ICT equipment which is removed from the admin offices for the purpose of class working or examination purposes and ensure staff are aware of the security requirements detailed in this policy
- ensure all staff, whether permanent or temporary, are instructed in their security responsibilities
- ensure staff using computer systems/media are trained in their use
- determine which individuals are given authority to access specific information systems. The level of access to specific systems should be on a job function need, irrespective of status
- ensure staff are unable to gain unauthorised access to college IT systems or manual data
- implement procedures to minimise the college's exposure to fraud, theft or disruption of its systems such as segregation of duties, dual control, peer review
- ensure current documentation is maintained for all critical job functions to ensure continuity in the event of relevant staff being unavailable
- ensure that the relevant system administrators are advised immediately about staff changes affecting computer access (e.g. job nature changes or leaving organisation) so that passwords may be withdrawn or changed as appropriate
- ensure that all contractors undertaking work for the college have signed confidentiality (non-disclosure) undertakings
- ensure the college's Clear Desk Policy is enforced, particularly in relation to confidential or personal information.
- ensure information held is accurate, up to date, and retained, in line with college retention and disposal procedures

- ensure relevant staff are aware of and comply with any restrictions specific to their role or work area.

Staff

Staff are responsible for:

- ensuring that no breaches of information security result from their actions
- reporting any breach, or suspected breach of security without delay. Further details can be found in the Incident Response Policy
- ensuring information, they have access to, remains secure. The level of security will depend on the sensitivity of the information and any risks which may arise from its loss.
- ensuring they are aware of and comply with any restrictions specific to their role or work area.

All staff should be aware of the confidentiality clauses in their contract of employment.

Advice and guidance on information security can be provided by HR, your line manager and, in relation to IT security, the IT Manager.

Part 1: Keeping Information Secure

Data Protection

The General Data Protection Regulation (GDPR) requires that organisations put in place appropriate technical and organisational principles and safeguard individual rights. This is known as 'data protection by design and by default'. This means that we have to integrate data protection into our processing activities and operations, from the design stage right through the lifecycle.

The college will, therefore, ensure that privacy and data protection is a key consideration in everything we do. As part of this we will:

- consider data protection issues as part of the design and implementation of systems, services, products and operations;
- make data protection an essential component of the core functionality of our processing systems and operations
- anticipate risks and privacy-invasive events before they occur and take steps to prevent harm to individuals
- only process the personal data that we need for our purpose(s) and that we only use the data for those purposes

Data Protection Impact Assessments (DPIAs) are an integral part of taking a privacy by design approach.

Data Breaches and Information Security Incidents

The college has a duty to ensure that all personal information is processed in compliance with the principles set out in the General Data Protection Regulation (GDPR). It is ultimately the responsibility of each Head of Operation (FE/HE) to ensure that their operation areas comply with that duty and that suitable procedures are in place for staff to follow when dealing with personal information.

Staff should be aware of requirements in relation to identifying and reporting security incidents and personal data breaches

Access control

Staff, students and contractors should only access systems for which they are authorised. Under the Computer Misuse Act (1990) it is a criminal offence to attempt to gain access to computer information and systems for which they have no authorisation. All contracts of employment should have a non-disclosure clause, which means that in the event of accidental unauthorised access to information (whether electronic or manual), the member of staff is prevented from disclosing information which they had no right to obtain.

Formal procedures will be used to control access to systems. An authorised manager must raise an Access Request to IT Manager for each application for access. Access privileges will be modified/removed - as appropriate - when an individual changes job or leaves. Managers must ensure they advise the IT manager of any changes requiring such modification/removal.

All Staff and students must comply with the college's ICT Policy in relation to passwords.

Where appropriate, staff working out notice are assigned to non-sensitive tasks or are appropriately monitored.

If an employee is leaving, particular attention should be paid to the return of items which may allow future access. These include but not limited devices, access codes, keys and documents.

Once an employee has left, it can be impossible to enforce security disciplines, even though legal process. Many cases of unauthorised access into systems and premises can be traced back to information given out by former employees.

System administrators will delete or disable all identification codes and passwords relating to members of staff who leave the employment of the college on their last working day. The employee's manager should ensure that all PC files of continuing interest to the business of the college are transferred to another user before the member of staff leaves.

Managers must ensure that staff leaving the college's employment do not inappropriately wipe or delete information from hard disks. If the circumstances of leaving make this likely then access rights should be restricted to avoid damage to college information and equipment.

All visitors should have official identification issued by the college. If temporary passwords need to be issued to allow access to confidential systems these need to be disabled when the visitor has left. Visitors should not be afforded an opportunity to casually view computer screens or printed documents produced by any information system without authorisation.

There is a requirement for system administrators to have a procedure in place for the secure control of contractors called upon to maintain and support computing equipment and software. The contractor may be on site or working remotely via a communications link. IT Manager will advise on the most suitable control.

Physical security to all office areas is provided through a sign-in and ID system. Staff should challenge strangers in the office areas without an ID badge.

Security of Equipment

Portable computers must have appropriate access protection, for example passwords and encryption, and must not be left unattended in public places.

Computer equipment is vulnerable to theft, loss or unauthorised access. Always secure laptops and handheld equipment when leaving an office unattended and lock equipment away when you are leaving the office.

Due to the high incidence of car thefts laptops or other portable equipment must never be left unattended in cars or taken into vulnerable areas.

Users of portable computing equipment are responsible for the security of the hardware and the information it holds at all times on or off college property. The equipment should only be used by the individual to which it is issued, be maintained and batteries recharged regularly.

Staff working from home must ensure appropriate security is in place to protect equipment or information. This will include physical security measures to prevent unauthorised entry to the home and ensuring college equipment and information is kept out of sight.

College issued equipment must not be used by non-college staff.

All of the policy statements regarding the use of software and games apply equally to users of portable equipment belonging to the college.

Users of this equipment must pay particular attention to the protection of personal data and commercially sensitive data. The use of a password to start work with the computer when it is switched on, known as a ‘power on’ password, is mandatory and all sensitive files must be password protected if encrypting the data is not technically possible. The new user will be provided with training session to learn how to apply these passwords, if required.

Users of portable equipment away from college premises should check their car and home insurance policies for their level of cover in the event of equipment being stolen or damaged and take appropriate precautions to minimise risk of theft or damage.

Security and Storage of Information

All information, whether electronic or manual, must be stored in a secure manner, appropriate to its sensitivity. It is for each department to determine the sensitivity of the information held and the relevant storage appropriate to that information. Suitable storage and security will include:

- Paper files stored in lockable cupboards or drawers
- Laptops or other portable equipment stored in lockable cupboards or drawers
- Electronic files password protected or encrypted
- Restricted access to ICT systems
- Computer screens to be 'locked' whenever staff leave their desk
- Removable media to be kept in lockable cupboards or drawers and information deleted when no longer required
- Laptops or other portable equipment must never be left in unattended vehicles
- At no time should sensitive, confidential or personal information be stored on a portable unit's hard drive.
- Staff should be aware of the position of their computer screens and take all necessary steps to prevent members of the public or visitors from being able to view the content of computers or hard copy information

Clear Desk Policy

Employees are required to clear working documents, open files, and other paperwork from their desks, working surfaces and shelves at the end of each working day and to place them securely into desk drawers and cupboards as appropriate.

Although security measures are in place to ensure only authorised access to office areas, employees should ensure that documents, particularly of a confidential nature are not left lying around.

Employees must ensure that documents are carefully stored. When properly implemented, this clear desk policy also improves efficiency as documents can be retrieved more easily.

Posting or Emailing Information

If information is particularly sensitive or confidential the most secure method of transmission must be selected.

Please consider the risk of harm or distress that could be caused to the customer if the information was lost or sent to another person, then look at the most appropriate way of sending the information to the recipient.

It is important that only the minimum amount of personal or sensitive information is sent, by whichever method is chosen.

The following procedures should be adopted as appropriate, depending on the sensitivity of the information.

Sending information by email:

- Carefully check the recipient's email address before pressing send – this is particularly important where the 'to' field autocompletes
- If personal or sensitive information is regularly sent via email, consider disabling the auto complete function and regularly empty the auto complete list. Both of these options can be found in Outlook under 'file', 'options' and 'mail'
- Take care when replying 'to all' – do you know who all recipients are and do they all need to receive the information you are sending
- If emailing sensitive information, password protect any attachments. Use a different method to communicate the password e.g. telephone call, messenger, or text
- Consider the use of secure email where this is available or use drop off and encrypt the document
- Person identifiable data files must not be sent via email to a user's personal mail box. Staff working from home should only access information via the college's network.

Sending information by post:

- Check that the address is correct
- Ensure only the relevant information is in the envelope and that someone else's letter hasn't been included in error
- If the information is particularly sensitive or confidential, discuss the most secure method of delivery with the Post Office, this could be by Special Delivery or even courier.

Printing and Photocopying:

- All printing must be via the college network printers
- Consideration must be given to using the Printers for large print runs, especially where personal information is concerned
- When printing or photocopying multiple documents, ensure you separate them when you return to your desk
- If the copier jams please remove all documents – if the copier remains jammed report it, but leave your details on the copier so that once it has been fixed any remaining copying can be returned to you. If possible, cancel your print run
- Make sure your entire document has copied or printed – check that the copier has not run out of paper. This is particularly important when copying or printing large documents. Please bear in mind the printer will sometimes pause in the middle of a large print run

- Do not leave the printer unattended when you're using it – someone else may come along and pick up your printing by mistake

Redacting

If it is necessary to redact information, either before sending it out or posting it onto the website, ensure a suitable and permanent redaction method is used

The use of black marker pen is not a suitable method of redaction

It is not advisable to change the colour of text (e.g. white text on a white background) or use text boxes to cover text as these can be removed from electronic documents. However, if this is the only option, once redacted the document should be printed and then scanned as a PDF before being sent.

Sharing and Disclosing Information

When disclosing personal or sensitive information to students, particularly over the phone or in person, ensure you verify their identity. Departments dealing with students on a daily basis should have suitable security questions which must always be used. If in doubt ask for suitable ID or offer to post the information (to the contact details you have on file) For the majority of information requests students will be required to submit a request form to which will then be processed along with appropriate checks

If a request for disclosure of information is received from a third party, you must:

- Obtain written consent from the customer that they are acting on their behalf
- verify their identity, particularly if they request information via the telephone or in person. It is preferable to telephone the person back, using a recognised telephone number for their organisation (for example 101 for the Police). Do not take their mobile number and use that.

In all circumstances, you must ensure you are legally able to share the information being requested and only share the minimum amount of information necessary.

Retention and Disposal of Information

Information must only be retained for as long as it is needed for business purposes, or in accordance with any statutory retention period

Staff should refer to the college's Data Retention Policy available in the Data Protection Policy for more details. This sets out the type of information held, together with statutory or agreed retention periods. Please contact the Published Information Panel for further advice on retention

When disposing of information please ensure the most appropriate method is used. Paper files containing personal or sensitive information must be shredded before disposal. Electronic information must be permanently destroyed

When purchasing new computer systems or software, please consider requirements for the retention and disposal of information and ensure these are included at the scoping stage

Vacating Premises or Disposing of Equipment

It is important that a process is in place to ensure all college information is removed from premises should they be vacated and from equipment before it is disposed of. Equipment includes cupboards and filing cabinets as well as computers or other electronic devices.

The disposal of computer or other electronic devices is referenced in this policy and all electronic equipment must be returned to be properly disposed of.

If the college vacates any of its premises, the manager of the premises must undertake appropriate checks of all areas, including locked rooms, basements and other storage areas, to ensure all college information is removed. Such checks should be documented, dated and signed.

If information is bagged for disposal (whether confidential or not), this must be removed before the building is vacated.

Cupboards and filing cabinets must be checked before their disposal to ensure they contain no documents or papers.

Part 2 – ICT Security

Cloud Storage Solutions

The use of cloud storage solutions (SkyDrive, Onedrive, iCloud etc.) for the transfer of student's personal information is expressly forbidden.

Systems Development

All system developments must comply with the college's IT Strategy. All system developments must include security issues in their consideration of new developments, seeking guidance from the IT Manager where appropriate.

Network Security

The college has processes in place for periodic reviews of network security. If any risk is trigged or highlighted by the system then IT manager conducts a detailed review.

Risks from Viruses

Viruses (including malware and zero-day threats) are one of the greatest threats to the college's computer systems. PC viruses become easier to avoid with staff aware of the risks with unlicensed software or bringing data/software from outside the college. Anti-virus measures reduce the risks of damage to the network. On lab PC's/students specified computers have deep freeze installed on them to counter any viruses and malware.

IT Services centrally maintain and update the currency of the virus definition files on servers, but users are responsible for checking that virus updates are automatically occurring on all desktop machines. Advice and support are available from IT Manager if any remedial action is necessary. Any suspected virus attacks must be reported to itsupport@edacollege.co.uk.

Cyber Security

Cyber security and cybercrime are increasing risks that, if left unchecked, could disrupt the day-to-day operations of the college.

The college has processes in place to ensure cyber security. If any risk is trigged or highlighted by the system then IT manager conducts a detailed network review for security.

Access Control to Secure Areas

Secure areas include:

- The filing rooms
- The archive rooms
- The ICT server room

The following access practices are in place

- All central processors/networked file servers/central network equipment will be located in secure areas with restricted access.
- The college's central computer suite is a high security area, an entry restriction and detection system are in place to protect the suite.
- Local network equipment/file servers and network equipment will be located in secure areas and where appropriate within locked room.
- Unrestricted access to the central computer facilities will be confined to designated staff whose job function requires access to that particular area/equipment.
- Restricted access may be given to other staff where there is a specific job function need for such access.
- All secure areas will have an entry log which staff and visitors must use.
- Regular reviews of who can access these secure areas should be undertaken.

Security of Third-Party Access

No external agency will be given access to any of the college's networks unless that body has been formally authorised to have access.

All external agencies will be required to sign security and confidentiality agreements with the college.

The college will control all external agencies access to its systems by enabling/disabling connections for each approved access requirement.

The college will put in place adequate policies and procedures to ensure the protection of all information being sent to external systems. In doing so, it will make no assumptions as to the quality of security used by any third party but will request confirmation of levels of security maintained by those third parties. Where levels of security are found to be inadequate, alternative ways of sending data will be used.

All third parties and any outsourced operations will be liable to the same level of confidentiality as college Staff.

Data Back-up

Data should be held on a network directory where possible, to ensure routine backup processes capture the data. Information must not be held on a PC hard drive without the approval of the IT Manager.

Data should be protected by clearly defined and controlled back-up procedures which will generate data for archiving and contingency recovery purposes.

Archived and recovery data should be accorded the same security as live data and should be held separately preferably at an off-site location. Archived data is information which is no longer in current use, but may be required in the future, for example, for legal reasons or audit purposes. The college's Data Retention Policy must be followed in determining whether data should be archived.

Recovery data should be sufficient to provide an adequate level of service and recovery time in the event of an emergency and should be regularly tested.

To ensure that, in an emergency, the back-up data is sufficient and accurate, it should be regularly tested. This can be done by automatically comparing it with the live data immediately after the back-up is taken and by using the back-up data in regular tests of the contingency plan.

Recovery data should be used only with the formal permission of the data owner

If live data is corrupted, any relevant software, hardware and communications facilities should be checked before using the back-up data. This aims to ensure that back-up data is not corrupted in addition to the live data. An engineer (software or hardware) should check the relevant equipment or software using his/her own test data.

Equipment, Media and Data Disposal

If a machine has ever been used to process personal data as defined under the Data Protection Act (2018) or 'in confidence' data, then any storage media should be disposed of only after reliable precautions to destroy the data have been taken. Procedures for disposal should be documented.

Many software packages have routines built into them which write data to temporary files on the hard disk for their own purposes. Users are often unaware that this activity is taking place and may not realise that data which may be sensitive is being stored automatically on their hard disk.

Although the software usually (but not always) deletes these files after they have served their purpose, they could be restored and retrieved easily from the disk by using commonly available utility software. Therefore, disposal must be arranged through IT Manager who will arrange for disks to be wiped or destroyed to the appropriate standards.

Software

Only licensed copies of commercial software are installed on each machine by IT department. It is a criminal offence to make/use unauthorised copies of commercial software and offenders are liable to disciplinary action. IT manager should ensure that a copy of each licence for commercial software is held. The loading and use of unlicensed software on college computing equipment is NOT allowed. All staff and members must comply with the Copyright, Designs and Patents Act (1988). This states that it is illegal to copy and use software without the copyright owner's consent or the appropriate licence to prove the software was legally acquired. The college monitors the installation and use of software by means of regular software audits; any breaches of software copyright may result in personal litigation by the software author or distributor and may be the basis for disciplinary action under the college's disciplinary and misconduct procedures.

If any user requires some specific software other than provided to be installed on their machine, he/she will formally request the IT Manager through their line manager. The college will only permit legally authorised software to be installed on its PCs.

Where the college recognises the need for specific specialised PC products, such products should be registered with IT department and be fully licensed.

Software packages must comply with and not compromise college security standards.

Computers owned by the college are only to be used for the work of the college. The copying of leisure software on to computing equipment owned by the college is not allowed. Copying of leisure software may result in disciplinary action. Computer leisure software is one of the main sources of software corruption and viruses which may lead to the destruction of complete systems and the data contained on them.

Educational software for training and instruction should be authorised, properly purchased, virus checked and loaded by IT Manager.

The college seeks to minimise the risks of computer viruses through education, good practice/procedures and anti-virus software positioned in the most vulnerable areas. Users should report any viruses detected/suspected on their machines immediately to IT Manager.

Use of Removable Media

It is the college's policy to prohibit the use of all unauthorised removable media devices. The use of removable media devices will only be approved if a valid teaching/training need is developed.

All staff, students and third parties must comply with the requirements regarding removable media which can be found in the ICT Policy.

Timeout Procedures

Inactive computers should be set to time out after a pre-set period of inactivity. Users must ‘lock’ their computers, if leaving them unattended for any length of time.

Good Practice Principles

- The College will identify its security risks and their relative priorities, responding to them promptly and confidently, implementing safeguards that are appropriate, effective, culturally acceptable and practical.
- To promote better sharing and exploitation of information, all College Information Users will have access to appropriate internal information, including overall guidelines to the security measures employed, wherever possible.
- All College Information Users will be accountable for their actions and all actions will be attributable to an identified individual.
- All information (including third party information) will be protected by safeguards and handling rules appropriate to its sensitivity and criticality.
- Information owners will generally be responsible for identifying to whom their information may be released. On occasions, current legislation or contractual obligations may require its disclosure to authorised external bodies such as the police or awarding body.
- The College will seek to ensure that its activities can continue with minimal disruption, or other adverse impact, should it or any of its locations or services suffer any form of disruption or security incident
- Actual or suspected security incidents must be reported promptly to the IT Manager who will manage the incident to closure and arrange for an analysis of lessons to be learnt.
- Documented procedures and standards, along with education and training, will supplement this Policy.
- Compliance with the Policy will be monitored on a regular basis by the IT Manager, which will review this policy annually for completeness, effectiveness and usability together with identification and approval of planned improvements during the following twelve months.

Policy Awareness

A copy of this Policy will be made available to all staff and students currently at the College, or when they join the College.

All Users are expected to be familiar with, and to comply with, the e-safety, computer facilities and Information Security guidelines at all times. Further information or clarification on any aspects of this Policy may be obtained from the IT Manager.

Appendix 1 - Anti-Virus Guidelines

What is a virus?

A computer virus is a damaging piece of software that can be transferred between programs or between computers without the knowledge of the user. When the virus software is activated (by incorporated instructions, e.g. on a particular date), it performs a range of actions such as displaying a message, corrupting software, files and data to make them unusable, and deleting files and/or data. While many of the viruses produced are benign and cause no real damage to the infected system, they always constitute a breach of security.

There is currently something like 60-75,000 known viruses and worms some 10-20 new viruses or variants appear a day. When a virus or worm is released into the public domain, network worms and mass mailer viruses can sometimes spread worldwide before anti-virus vendors have had time to produce updates. *(A worm is a self-replicating virus that does not alter files but resides in active memory and duplicates itself. Worms use parts of an operating system that are automatic and usually invisible to the user. It is common for worms to be noticed only when their uncontrolled replication consumes system resources, slowing or halting other tasks)*

Even daily anti-virus updates are not always enough to ensure safety from all possible threats.

What does the college's IT Services do to prevent the spread of viruses?

Whilst precautions are taken at the network level to minimise the spread and impact of worms and viruses, it is not possible to make the process totally effective. Protection from viruses and worms is not a process that can be left entirely to system administrators, IT Manager, and anti-virus software. The best efforts of administrators and IT manager are not sufficient - all computer users must also play their part by taking simple precautions like those described below.

Avoid Unauthorised Software

Programs like games, joke programs, cute screensavers, unauthorised utility programs and so on can sometimes be the source of difficulties even if they are genuinely non-malicious. That is why it is forbidden to install them. If such programs are claimed to be some form of antivirus or anti-Trojan 2 utility, there is a high risk that they are actually in some way malicious! *(In computers, a Trojan horse is a program in which malicious or harmful code is contained inside apparently harmless programming or data in such a way that it can get control and do its chosen form of damage. In one celebrated case, a Trojan horse was a program that was supposed to find and destroy computer viruses. A Trojan horse may be widely redistributed as part of a computer virus.).*

Treat all attachments with caution

It makes sense to be cautious about email attachments from people you don't know. However, if attachments are sent to you by someone you do know, don't assume they must be OK because you trust the sender.

Worms generally spread by sending themselves without the knowledge of the person from whose account they spread. If you do not know the sender or are not expecting any messages from the sender about that topic, it is worth checking with the sender that they intended to send a message, and if so, whether they intended to include any attachment. If you were expecting an attachment from them, this may not apply.

However, one recent virus sends out an email telling you that a ‘safe’ attachment is on the way, then sends out mail with a copy of itself as an attachment.

Bear in mind that even legitimate, expected attachments can be virus infected: worms and viruses are related, but cause slightly different problems.

Regard anything that meets the following criteria with particular suspicion:

- If they come from someone you don't know, who has no legitimate reason to send them to you.
- If an attachment arrives with an empty message.
- If there is some text in the message, but it doesn't mention the attachment.
- If there is a message, but it doesn't seem to make sense.
- If there is a message, but it seems uncharacteristic of the sender (either in its content or in the way it's expressed).
- If it concerns unusual material like pornographic web-sites, erotic pictures and so on.
- If the message doesn't include any personal references at all, (for instance a short message that just says something like "You must take a look at this", or "I'm sending you this because I need your advice” or “I love you!").
- If the attachment has a filename extension that indicates a program file (such as those listed below).
- If it has a filename with a ’double extension’, like FILENAME.JPG.vbs or FILENAME.TXT.scr, that may be extremely suspicious. As far as Windows is concerned, it's the last part of the name that counts, so check that against the list below to find out whether it's a program like those listed, masquerading as a data file, such as a text file or JPEG (graphics) file.

In all the above instances, it is recommended that you check with the sender that they knowingly sent the mail/attachment in question.

Avoid unnecessary macros

If Word or Excel warn you that a document, you're in the process of opening contains macros, regard the document with particular suspicion unless you are expecting the document and you know that it's supposed to contain macros. *(In Microsoft Word and other programs, a macro is a saved sequence of commands or keyboard strokes that can be stored and then recalled with a single command or keyboard stroke. A macro virus is a computer virus that "infects" a Microsoft Word or similar application and causes a sequence of actions to be performed automatically when the application is started or something else triggers it.)*

Even then, don't enable macros if you don't need to. It may be worth checking with the person who sent it to you that it is supposed to contain macros.

Be cautious with encrypted files

If you receive an encrypted (passworded) attachment, it will normally be legitimate mail from someone you know, sent intentionally (though the sender is unlikely to know in the event that they have a virus). However, that doesn't necessarily mean that it isn't virus-infected. If it started out infected, encryption won't fix it. Furthermore, encrypted attachments can't usually be scanned for viruses in transit: the onus is on the recipient to be sure the decrypted file is checked before it's opened. This goes not only for heavyweight encryption packages, but also for files compressed and encrypted with PKZip or WinZip.

Suspicious filename extensions

The following is a list of filename extensions that indicate an executable program, or a data file that can contain executable programs in the form of macros. This list is by no means all-inclusive. There are probably a couple of hundred filename extensions that denote an executable program of some sort. *(An executable is a file that contains a program. It is a particular kind of file that is capable of being executed or run as a program in the computer. In a Windows operating system, an executable file usually has a file name extension of .bat, .com, or .exe)*

Furthermore, there are filenames like .RTF that shouldn't include program content, but sometimes can, while Word documents (for instance) can in principle have any filename extension, or none. Furthermore, zipped (compressed) files with the filename extension .ZIP can contain one or more of any kind of file.

. BAT .CHM .CMD .COM .DLL .DOC .DOT
.EXE .FON .HTA .JS .OVL .PIF .SCR
.SHB .SHS .VBS .VBA .WIZ .XLA .XLS

Report it!

If you think that you may have received a virus - report it!

Appendix 2 - Cyber Security Approach

Introduction

This document identifies the risks to the college from main threats of cyber security and sets out what is in place to mitigate these risks.

If you do not understand anything in this document or feel you need specific training you should bring this to the attention of your line manager.

Purpose and Objectives

The document provides guidance to staff and members on the risks that threats from cyber security pose to the college.

In addition, the following policy is relevant to all staff and have some impact on the threats from cyber security:

- ICT Policy

Roles and Responsibilities

The IT Manager is responsible for the provision of the appropriate technology and technological devices to ensure that the college is reasonably protected from the threats from cyber security.

The college is responsible ensuring that staff are communicated with about how to ensure that they don't put the college at risk.

All staff and students should not take any action that puts the colleges systems or information at risk from cyber security. Any incidents must be reported in line with the Information Security policy.

Cyber Security

Cyber security and cybercrime are persistent threats that, if left unchecked, could disrupt the day to day operations of the college, the delivery of local public services and ultimately have the potential to compromise national security. Additional costs will be incurred by the college to rectify any cyber security or cybercrime event.

Technical advances create opportunities for greater efficiency and effectiveness. These include more engaging and efficient digital services, new ways to work remotely and to store and transfer data, such as mobile devices and cloud services.

The scale of targeted attacks, coupled with the difficulty of monitoring all possible attack methods requires the public sector to work together to both reduce the likelihood and the impact of such a threat succeeding.

Foreign states, criminals, hacktivists, insiders and terrorists all pose different kinds of threats. They may try to compromise public sector networks to meet various objectives that include:

- Stealing sensitive information to gain economic, diplomatic or military advantage over the UK
- Financial gain

- Attracting publicity for a political cause
- Embarrassing central and local government
- Controlling computer infrastructure to support other nefarious activity
- Disrupting or destroying computer infrastructure

College employees can also be targets for criminal activity.

Cyber Security Risks

The following types of cyber security all pose risks to the college:

Cybercrime:

The most common form of cyber-attack against public bodies is the use of stolen or false customer credentials to commit fraud.

The uptake in online services means this form of crime can now be undertaken on a much larger scale and can be international.

Cybercriminals also seek to steal data from government networks that has a value on the black market, such as financial information or data that can be used for ID theft.

There are several types of malware (malicious software) that have been written to specifically steal banking and log in information.

The college secures its network with up-to-date antivirus and malware protection, and manages the use of personal USB devices on college computers.

Hacktivism:

Hacktivists seek to cause embarrassment or annoyance to the owners of high- profile websites and social media platforms that they may deface or take off line.

When targeted against local government websites and networks, these attacks can cause reputational harm both locally and nationally.

The college has third party availability monitoring tools in place to alert key team members of the website's status.

The college's web site's content management system conforms to the colleges
ICT Policy with regards to password enforcement.

Insider threats:

An insider is someone who exploits, or intends to exploit, their legitimate access to an organisation's assets for unauthorised purposes. Such activity can include:

- Unauthorised disclosure of sensitive information
- Facilitation of third-party access to an organisation's assets
- Physical sabotage
- Electronic or IT sabotage

Not all insiders deliberately set out to betray their organisation. An unwitting insider may compromise their organisation through poor judgment or due to a lack of understanding of security procedures.

The insider threat is not new, but the environment in which insiders operate has changed significantly. Technology advances have created opportunities for staff at all levels to access information.

The college enforces the use of strong passwords for access to systems. The college prohibits the use of personal USB devices.

The college periodically reviews access to key IT systems.

Physical Threats:

The increasing reliance on digital services brings with it an increased vulnerability in the event of a fire, flood, power cut or other disaster natural or otherwise that could impact upon local government IT systems.

The college has a disaster recovery (DR) and business continuity (BC) data centre for its core services.

Terrorists:

Some terrorist groups demonstrate intent to conduct cyber-attacks, but have limited technical capability. Terrorist groups could acquire improved capability in a number of ways, namely through the sharing of expertise in online forums providing an opportunity for escalations and the hiring of Hacktivists.

Espionage:

Several of the most sophisticated and hostile foreign intelligence agencies target UK government and public sector networks to steal sensitive information. This could ultimately disadvantage the UK in diplomatic or trade negotiations.

The college's approach to Cyber Security

As with most educational Institutions, the college relies heavily on access to the internet and to information held in its systems. There are several IT systems that have an internet presence (website, webmail, homeworking), and there are several different access mechanisms to information (Wi-Fi, physical networking, smartphones, tablets). All present threats to cyber security. It is widely acknowledged that it is not currently possible to keep out all attacks all of the time, but the college employs a range of tools and good practice to minimise the risk to its information and systems.

The college has clear policed on ICT and Information Security, which provide information on a range of areas including:

- Reporting of security incidents
- Use and security of emails
- Use of the internet
- Mobile phone usage
- Passwords

- Removable Media
- Clear desk policy
- Sharing and disclosing information
- Cloud storage systems
- Viruses
- Equipment, media and data disposal

The college employs a range of technology and processes to help it achieve a good security platform. These range from up-to-date firewalls and core networking equipment, through antivirus controls and a secure wireless configuration, to encrypted devices and mobile device management.