# IT SECURITY POLICY

| Document Control | |
|---|---|
| Manager responsible | Tina Tupper, ILT Manager |
| Version number | 4.0 |
| Approved by | SLT |
| Approval date | 07 October 2020 |
| Review date | October 2021 |

# IT SECURITY POLICY

Contents

## Introduction

Hereford College of Arts has a large investment in the use of Information Technology (IT) which is used to the benefit of all departments, students and Governors (users). In many areas of the College the use of IT is vital and must be protected from any form of disruption or loss of service. It is, therefore, essential that the availability, integrity and confidentiality of the IT systems and data are maintained at a level which is appropriate for HCA needs.

In this policy, 'IT security' is defined as:

*the availability,*

This means that information and associated assets should be accessible to authorised users when required and therefore physically secure. The computer network must be resilient, and HCA must be able to detect and respond rapidly to incidents (such as viruses and other malware) that threaten the continued availability of assets, systems and information. HCA has appropriate business continuity plans (outlined below in section 16).

*confidentiality*

This involves ensuring that information is only accessible to those authorised to access it and therefore to preventing both deliberate and accidental unauthorised access to HCA's information and proprietary knowledge and its systems including its network, website, and intranet.

*and integrity*

This involves safeguarding the accuracy and completeness of information and processing methods, and therefore requires preventing deliberate or accidental, partial or complete, destruction or unauthorised modification, of either physical assets or electronic data. There is appropriate contingency *including for network, website and intranet* and data backup plans and security incident reporting. HCA complies with all relevant data-related legislation in those jurisdictions within which it operates.

*of the physical (assets)*

The physical assets of HCA including, but not limited to, computer hardware, data cabling, telephone systems, filing systems and physical data files.

*and information assets*

The information assets include information printed or written on paper, transmitted by post or shown in films, or spoken in conversation, as well as information stored electronically on servers, website, intranet, PCs, laptops, mobile phones and PDAs, as well as on CD ROMs, floppy disks, USB sticks, backup tapes and any other digital or magnetic media, and information transmitted electronically by any means. In this context, 'data' also includes the sets of instructions that tell the system(s) how to manipulate information (i.e. the software: operating systems, applications etc.)

## 1. Policy Objectives

There are three main objectives of this policy:

- to ensure that all of HCA assets, users, data and equipment are adequately protected against any action that could adversely affect the IT services required to conduct our business;
- to ensure that users are aware of and fully comply with all relevant legislation.
- to create and maintain, within all areas, a level of awareness of the needs for IT security to be an integral part of our day to day operation so that all users understand the need for IT security and their own responsibilities.

## 2. Application

The security policy is relevant to all IT services irrespective of the equipment or facility in use and applies to:

- All HCA users
- Staff, students and representatives of other organisations who directly or indirectly support or use the IT services.
- All use of IT throughout HCA and its satellite sites.

## 3. Responsibility for Security

- IT security is the responsibility of HCA as a corporate entity and all users. The policy has been approved and adopted by the Senior Leadership Team (SLT) and the College Corporation.

- The IT security policy will apply to all users who use computer facilities whether they are networked or standalone PCs. All users are to be issued with computer security instructions or informed of where copies can be obtained, which specify their responsibilities and draw their attention to the penalties for not complying with the instructions.

- The Wider Leadership Group must be responsible for the implementation of the Security Policy and will receive procedural notes to cover the key areas of responsibility during the induction process.

- All providers of the IT services must ensure the security, integrity and availability of the data within the service provided.

## 4. Personal Devices

Staff and students are permitted to utilise their own mobile devices within the college. The devices must only connect using the Eduroam Wi-Fi provided logging on with the credentials given to individuals during the induction process.

Staff and students must take full responsibility for the care of their devices and ensure that personal insurance policies cover the use of the device within the college campus.

Although every effort is made to support the wide variety of operating systems devices may use, the college is unable to guarantee connection of the device to the Wi-Fi facility.

IT staff are not able to support staff or students with any technical issues they may have with their personal devices. Individuals are advised to contact the vendor for after sales service.

Under no circumstances must a personal device be directly connected to the HCA Network.

Although HCA make every effort to provide a safe network for personal use persons connecting their own devices to our systems do so at their own risk.

## 5. Portable Devices & Removable Media

**Note: HCA will not permit any data that may be considered sensitive or could compromise Data Protection to be stored on portable devices. HCA considers cloud storage to be the safer option.**

Portable devices such as Tablets, Laptops, Smart Phones, external HDD, USB devices and CD/DVD, should be password protected to ensure the safety of the data stored on them.

What is 'removable media'? Although most of this document refers explicitly to USB sticks the policy covers any means of data storage that can be used for taking electronic information from HCA systems. This includes, but is not limited to, CD and DVD burning. Also, many consumer electronics gadgets such as PDAs, Blackberries, iPods and phones can be used for removable data storage.

### What are memory sticks?

USB sticks are small yet capacious. Their size makes them convenient to carry but also makes them easy to have stolen or to lose. A memory stick can contain thousands of documents and large databases. Whole directories can be put onto a stick without checking exactly which files are being copied and what their individual security classification is. It is also possible that if the stick is taken away and used on a virus infected PC, many corrupted documents may then be put back onto the HCA network. At the very least you could lose a vital document. It's also worth remembering that these sticks can, on occasion, fail and information may be lost. USB sticks must only be used for the temporary transfer of documents.

### Rules about memory stick use

- Ensure that portable storage devices are not being used to store sensitive, confidential or personally identifiable information without prior consultation with IT Department. IT technical staff can advise on adding a high level of security to the device.
- Ensure that portable devices are stored securely when left unattended.
- Devices taken off-site should not be left unattended in public places or at individual's home address.

- Ensure that information held on portable storage devices is not automatically copied (backed-up). To avoid total loss of data, users must ensure that information stored on portable storage devices is 'backed-up' and held in the appropriate place on the HCA Network or cloud services.
- If a portable storage device is lost, stolen or mislaid it must be reported immediately to your line manager and the IT Department.
- Staff are responsible for ensuring that visitors or contractors who bring their own USB devices into the HCA (to give a presentation for example) are always supervised whilst the device is connected to HCA equipment.
- HCA PCs automatically scan USB memory sticks for potential viruses. However, staff are responsible for scanning when off site. The device should be used carefully and use in untrusted PCs should be avoided.

In short, if you need to take any information from the HCA network out of HCA consider whether the information would be damaging to the HCA if it was lost. If so, please contact the IT Department for advice on the safest way to proceed.

## 6. Legislation

HCA must abide with all UK legislation affecting IT. All HCA users must comply with the following Acts and may be held personally responsible for any breach of current legislation as listed below and any future legislation that may be enacted.

- Data Protection Act 2018
- Copyright, Designs and Patents Act 1988
- Computer Misuse Act, 1990
- Malicious Communications Act 2003
- Counter-Terrorism and Security Act 2015
- Police and Justice Act 2006
- Regulation of Investigatory Powers Act 2000Digital Economy Act 2017

## 7. Standards and Procedures

Physical access

Precautions should be taken to ensure access to PCs is always restricted to authorised personnel only.

Equipment should be sited to reduce the risk of fire, damage, interference and unauthorised access.

All computer equipment must be security marked and be audited on the Information Technology (IT) inventories.

Where computer equipment needs to be moved e.g. change of office/for use at home:

- Prior approval in writing must be obtained from Course Leaders specifying the reason for the removal and the duration and submitted to the IT Network Manager for approval on behalf of SLT. Appropriate mechanisms should be employed by the IT Network Manager on behalf of SLT & CL'S to ensure the timely return of loaned Computer equipment and that no damage has occurred. Short term loans of laptops and peripherals are managed by the *IT department* using the Wasp Barcode system for logging the details of the equipment and duration of the loan.

- All provisions of this policy document equally apply.

No equipment purchased, leased or hired by a user may be connected to the network or attached to any equipment connected to the network without authorisation from the IT Network Manager. This restriction also applies to any equipment not owned, leased or hired by HCA.

## 8. User Management

Student User Accounts are created by importing from REMS Registry System and enabled after completion of the IT H&S process. Student Accounts are deleted when completed or withdrawn. The Registry team alert the IT team as and when these occur.

Staff User Accounts are created once the recruitment process has been completed. this requires a clear DBS check or risk assessment and a completed Computer Access Form by the Line Manager. Staff are required to complete an IT H&S Induction and have a face to face inductions with a member of IT staff to ensure they understand the systems they are required to use. Staff accounts are disabled by instruction from Personnel.

### Third party user management

All external suppliers who have access to HCA's I.T. Systems or data must work under the supervision of college staff and in accordance with this Policy. A copy of the Policy will be made available to the supplier, if required.

## 9. Remote Access

All users of the HCA systems are expected to comply with the IT Security Policy whether working Remotely or on site. Particular attention should be taken when setting up space for work ensuring the space is suitable for conducting online meetings and is secure when data is stored. Staff are advised to follow the Working From Home guidelines available on StaffNet.

## 10. Software Access

Requests to provide access to the network for staff should be made in writing, in advance, to the I.T. Manager by a member of Senior Management Team or the Personnel Officer. In the case of students this will be done via the normal induction procedure.

PCs should not normally be left "logged in" when unattended. Where this does occur, it should be ensured that the desktop is locked by the user and where it can be only unlocked by that user or an IT Administrator. In addition, all offices should be locked when unattended to provide security to hardware and devices.

Passwords should be used to protect all systems and should not be written down or disclosed to others. Users will be held liable for any misuse of a computer resulting from use of their password/username. Staff or students should not log in to the system for any other person.

Staff Passwords should be changed every 90 days and Student Passwords are changed by the individual as and when it is required.

Passwords should normally be specific to individuals and comprise of a minimum of 8 characters to include 3 of the 4 following characters; uppercase, lowercase, number and/or symbol arranged in such a fashion, as they will not easily be guessed.

## 11. Information

Information held on HCA's IT facilities or subsequent output, e.g. printed letters etc., is the property of HCA and is governed by the provisions of the Data Protection Act. The nominated Data Protection person must register any purpose for which personal information is held about people under the act.

Information held should only be released to authorised persons and IT facilities supplied must only be used for authorised purposes. Where IT facilities are used for personal work this activity must not prejudice or interfere in any way with either the HCA IT facilities or its business activities.

Any personal or sensitive data displayed upon unattended equipment must be protected, particularly in a public area, to ensure it may not be seen by anyone unauthorised to do so. This is applicable to information displayed on PCs, printed output and computer produced media such as OHP slides.

All computer output no longer required by HCA staff should be disposed of with due regard to its sensitivity. Confidential output should be disposed of by shredding.

Any queries relating to the provisions of the Data Protection Act and how it affects your operations should be directed to SLT.

Essential information must be stored on the Network to ensure daily back-ups are taken. Essential information should not be stored on local hard drives or 3rd party devices where back-ups are not taken and data is not retrievable by the restore process.

## 12. Virus protection

All Networked PC's have antivirus software installed and the software updated automatically on a daily basis. All PCs (including laptops/notebooks) must be protected by virus detection software and upgraded on a regular basis to guard against new viruses. Any detected viruses must be reported to IT immediately.

All external devices are virus checked upon access. This is essential when devices have been received from an external source. In the case of Email and attachments, from an unknown external source, extra care must be exercised. If in doubt do not open the Email and contact IT Support.

Disks/CD-ROMs/USBs or other external data devices must not be inserted into PCs until the computer has either reached:

- The point where you have logged into the network, or
- The Windows/Mac OS screen on stand-alone computers.

## 13. Cyber Security

Users should be vigilent and aware of potential threats from Phishing and Hacking whiles using HCA systems whether remote working or on site. All potential threats should be reported to the Network Manager immediately.

## 14. Software copyright

The copying of proprietary software programs or associated copyrighted documentation is prohibited and is an offence and could lead to personal criminal liability with the risk of a fine or imprisonment.

The loading of proprietary software programs for which a license is required but not held is prohibited and this is also an offence, which could lead to a large fine or imprisonment. All software system disks, and license should be held by IT.

Personal software should not be loaded onto HCA computers under any circumstances. If the software is deemed to be of use to HCA, then it should be duly acquired under license.

The loading of any software onto HCA computers is the responsibility of the IT department and requests should be made in writing to IT Support.

All end users other than IT Technical staff do not have the ability to install software on individual machines. End users requiring specific software must make a request to ILT Manager to ensure End User Agreements are being met. Site licences allow unlimited installations for Microsoft Office and Adobe software and are managed by IT staff.

## 15. Computer misuse

All users should be aware of their access rights for any given hardware, software or data and should not attempt to access hardware, software or data for which they have no approval or need to conduct their duties.

All users must read and agree to the Hereford College of Arts Acceptable Use Policy and E-safety policy during the induction process before being granted access to the Network.

## 16. Contingency planning

Security copies (back-ups) should be taken at regular intervals dependent upon the importance and quantity of the data concerned and in accordance with the HCA Back-up Policy. In the case of systems operations on the network these will be taken on behalf of users by IT at frequencies agreed with SLT.

In the case of networked computers, the master copy of all data files must be held on the network file server(s).

In the case of stand-alone computers, users should be aware that disks are susceptible to failure and should hold a copy of all data files on a back-up media.

Arrangements must be made by SLT & CL'S in conjunction with the IT Network Manager, for critical systems/operations to continue in the event of complete computing failure.

Security copies should be stored away from the system to which they relate, ideally, in restricted access fireproof locations. Security copies should be regularly tested to ensure that they enable the system/relevant file to be re-loaded in an emergency.

Security copies should be clearly marked as to what they are and when they were taken. Depending upon the system concerned they should provide for system recovery at various points in time over a period of several weeks.

Termly partial restore of systems will ensure systems can be restored from back-up in the case of a disaster recovery.

## 17. Acquisition and Disposal of IT

All acquisitions should be in accordance with the provisions of HCA strategy and its financial regulations. Any queries should be directed to the Finance Director (FD).

The disposal or permanent hand over of equipment, media or output containing personal or sensitive data must be arranged to ensure confidentiality.

Disposal of any PCs should only be carried out by IT Support who should be consulted to arrange for the permanent removal of all data and programs unless the recipient is taking over the software license or is authorised to use it.

Disposals should be in accordance with the provisions of the financial regulations, and the College disposal policy. Disposals will be conducted by IT.

Asset schedules or inventories held by Finance and IT must be updated to reflect the disposal.

WEEE (Waste Electrical and Electronic Equipment) Certification shall be obtained from the Disposal company in accordance with the The Waste Electrical and Electronic Equipment Regulations 2013.

## 18. Suspected security incidents

It is the duty of all users to report any suspected irregularities/fraud to SLT & the ILT Manager as soon as possible. All users involved shall regard such information as confidential.

## 19. Violations

Violations of this security policy may include, but are not limited to, any act that:

- Exposes HCA to actual or potential monetary loss through the compromise of IT security.
- Involves the disclosure of confidential information or the unauthorised use of corporate data.
- Involves the use of data for illicit purposes, which may include violation of any law, regulation, or any reporting requirement of any enforcement or government body

Any individual who has knowledge of a violation of this IT security policy must report that violation immediately to the ILT Manager.