P O L I C Y

TITLE:	Data Handling, Security and Communications
AIM:	To ensure that all users of College ICT systems understand the way in which their personal information is processed, their obligations under the General Data Protection Regulation (GDPR) and the protocols and principles governing the processing. security and communication of College Data and the ICT systems use in its storage and processing.
RELATED POLICIES & PROCEDURES:	• DBS Code of Practice • Disclosure Policy • Disciplinary Policy • Employment Reference Policy • ICT Acceptable User Policy • Archive and Retention Policy • ICT Disaster Recovery Policy • Freedom of Information Publication Scheme • Safeguarding Children and Vulnerable Adults Policy • CCTV Scheme • CCTV Code of Practice
DATE FOR IMPLEMENTATION:	*As Date of Approval*
APPROVED BY:	• Directorate 29-Jan-18 • JCNC 21-Feb-18 • RF & HR Committee 14-Mar-18
DATE OF APPROVAL:	14 March 2018
DATE OF NEXT REVIEW:	March 2021
DISTRIBUTION:	All Staff via Intranet
VERSION CONTROL:	*Version 2* *Last approved version: 15 March 2017*
PERSON RESPONSIBLE:	*Director of Human Resources*

EQUALITY IMPACT ASSESSMENT		
Phase 1 **Initial Screening completed**	**Date:**	September 2011
Phase 2	✓ **Not required**	*(please tick if appropriate)*

Full impact assessment completed/ not required	Completed on *(if applicable):*	
This document is available in alternative formats, please contact reception or, alternatively, e-mail info@eastridingcollege.ac.uk to discuss how we can help you.		

1. Statement of Intent/Scope and Purpose

East Riding College ("the College") collects, stores and processes personal information about its learners and members of staff. The College manages personal and sensitive information in both electronic and paper form and there is an increasing requirement to process electronic financial information such as credit and debit card transactions.

The College delivers remote web based services and VPN services to users, providing them with access to college data resources, Web based email and the Moodle VLE. These services must be delivered in a secure environment.

The PCI Data Security Standard defines the specific compliance requirements the college must meet in order to carry out both online and offline credit/debit card transactions.

The General Data Protection Regulation (GDPR) imposes certain obligations on the College relating to the way in which it deals with sensitive and personal information. As an organisation using the Disclosure and Barring Service ("DBS") to help assess the suitability of applicants, the College is required to comply with the DBS Code of Practice regarding the correct handling, use, storage, retention and disposal of disclosure information.

To ensure that data is managed securely and responsibly this policy defines the key principles relating to the processing, security and communication of data within the college.

This policy is applicable to all data and information held by the College and paper based systems including but not restricted to: desktop computers, network servers, portable equipment, electronic data, paper files, hardcopy and logs.

This policy informs staff and learners of the way in which their personal information is handled and explains the obligations of the College, its staff and learners under the applicable Law. One of the most important obligations is that personal information must be safeguarded against unauthorised or unlawful processing and against accidental disclosure, loss, destruction or damage. This means that the College, staff and learners must take appropriate measures to ensure that personal information is kept secure with access strictly controlled and limited to those who are entitled to access it as part of their duties. This policy defines the responsibility of staff and learners for ensuring that any personal data they provide to the College is up-to-date and accurate and that they inform the College of any changes to the data they have provided.

2. Responsibilities

The College Data Protection Officer is responsible for ensuring that the College complies with the General Data Protection Regulation (GDPR), Freedom of Information Act 2000 and the DBS Codes of Practice. Staff and learners will receive additional training in respect of the College's data handling and security procedures.

The Director of Human Resources and the Director of Learner Services, Planning and Diversity are responsible for ensuring secure transmission of College data to partner organisations.

The ICT Manager is responsible for providing help and guidance on all matters relating to information security and is responsible for ICT Systems Security.

The Director of Learner Services, Planning and Diversity, Facilities Manager and ICT Manager are responsible for the specification and management of on-line, cloud based electronic data archiving systems used by the College.

The Client Services & Enrichment Manager is responsible for providing up-to-date information on safeguarding requirements and current issues relating to on-line safety.

The Finance Manager is responsible for ensuring that financial transactions are carried out securely and that the College complies with the Payment Card Industry Security Standard (PCI DSS).

The Facilities Manager is responsible for the safe and secure storage and disposal of classified paper based materials.

All managers are responsible for ensuring compliance with this policy within their operational areas.

Key management responsibilities are:

- Compliance with GDPR legislation.
- Ensuring that the ICT Security Procedures are followed.
- Ensuring data (electronic and hard copy) and equipment disposal is carried out according to College policy. The policy for the safe destruction and disposal of electronic data is contained in section 5.11.of this document.
- Ensuring members of staff are instructed in their security responsibilities, including implementing password control, home and off-site working, transmission and movement of sensitive and personal data.
- Ensuring members of staff are aware of the confidentiality clauses in their contract of employment
- Ensuring that the relevant managers are advised immediately about staff changes affecting computer access or breaches of security protocols

3. Considerations for Policy

The College's security measures must operate within the following framework:

1. Responsibility – ensuring that there is a clear line of responsibility for data security within senior management and that all users of College ICT systems are aware of their responsibility relating to data security

2. Classification – ensuring all data and information is classified to protect it from unauthorised use and disclosure

3. Integrity – ensuring that data and information is safe, accurate and current and has not been deliberately or inadvertently modified from a previously approved version

4. Physical Security – ensuring that all data and information storage and retrieval systems are physically secure and cannot be removed from College property without the appropriate directorate level authority

5. Storage, Disposal and Transmission – ensure that the movement and disposal of all data and information is controlled according to its classification and that appropriate encryption methods are used to secure sensitive data and information

The following legislation and published standards are applicable to this policy:

- General Data Protection Regulation (GDPR)
- Freedom of Information Act 2000
- PCI Data Security Standard (PCI DSS)
- DBS Code of Practice

4. Risk Assessment

Failure to comply with this policy may result in the College contravening its legal responsibilities and being exposed to severe financial penalties and potential criminal/civil proceedings.

5. Policy

5.1 Processing Personal Information

The College has a legal obligation to ensure that staff and, in certain circumstances, learners are suitable to have contact with minors and vulnerable adults. The College must also take reasonable steps to ensure that staff, learners and other users of the College's facilities do not pose a threat to the health and safety of others. Accordingly, the College will process personal information as it requires in order to safeguard those to whom a duty of care is owed. This may include obtaining information about staff and learners from third parties.

Staff and Learners should ensure that the College is made aware of any medical condition along with relevant information about their medication. This information will be used to protect their health and safety and the health and safety of others.

The College carries out appropriate checks via the Disclosure and Barring Service (DBS) to ensure the safety of College learners, staff and visitors. On receipt of a DBS check, HR will record the following information:

- Employees name
- Post title
- Type of disclosure
- Date of issue
- Unique reference number

This information is verified by a second signatory, and the DBS certificate is returned to the employee and the relevant information is stored within HR. If details of a criminal conviction are recorded on the DBS, a risk assessment will be carried out by HR, following which the DBS certificate is confidentially destroyed.

5.2 Classification

The classification of data and information will be carried out according to the following guidelines:

Unrestricted	Public information (including information deemed public by legislation or through a policy of routine disclosure). Data in this category can be made freely available the public, all employees, College learners, contractors and agents. For example; the college prospectus.
Protected	Data that is sensitive outside the College and needs to be protected. Authorised access must be granted by the appropriate manager to this information on a 'need to know' basis for business related purposes. For example; what the college pays for business services such as Internet connectivity.
Confidential	Information that is sensitive within the College and is only available to a specific business function, group or role. For example; personal details relating to a staff member or learner.
Restricted	Information that is highly sensitive within the College and is only available to specific individuals with the express written authority of the Principal or Governing Body. For example; Salaries, network administration level credentials.

5.3 Integrity of Data

All users of College ICT systems are responsible for the integrity of information and data under their control.

Any information that is necessary to process credit/debit card transactions correctly is stored securely. Card verification and security codes must only be stored on secure and encrypted systems, it is forbidden to keep paper copies.

Staff, Learners and Contractors should only access systems for which they are authorised. Access privileges will be modified or removed, as appropriate, when an individual changes or leaves their employment at the College.

Any information both electronic and hard copy, to be shared or used outside of the College which contains personal or sensitive information must be covered by an appropriate Data Sharing Contract, ensuring compliance with GDPR requirements. Any member of staff submitting electronic information to external partners under the arrangements agreed in a Data Sharing Contract must ensure that files are fully encrypted or password protected and that notification of passwords is secure. Third party processors must process data in accordance contract terms.

No College data or electronic documents containing sensitive personal data or corporate information that would damage the reputation of the College or expose the College to legal action should it be lost, may be transmitted electronically, copied to removable media or portable devices without the express written consent of a College Data Protection Officer unless recorded on the Data User Manifest. Under no circumstances may non-encrypted sensitive data be removed from College premises either physically or by electronic transmission. All staff issued with portable devices capable of storing electronic data, will be trained on how to encrypt or password protect such data and will be required to do so

before removing the device from the College. Failure to comply may lead to disciplinary action.

Staff, Learners and Contractors must not disclose sensitive personal information to any third party, or even to the person to whom it relates, except in accordance with this Policy and the College's authorised procedures. Data Subjects may request their own personal data through a Subject Access Request.

All key systems should be adequately documented by the relevant systems manager. Such documentation should be kept up to date so that it matches the state of the system at all times. System documentation, including manuals, should be physically secured when not in use. Disaster recovery manuals, procedures and documentation issued to ICT Support Staff will be stored on encrypted USB sticks.

The College reserves the right for appropriately authorised staff to examine any data including personal data held on College systems or, when operationally necessary, for example to give supervised access to a private user account to a line manager or colleague. Certain staff within the College have been authorised to examine files, emails and data within individual accounts, but will only do so when operationally necessary.

When a member of staff leaves the employment of the College their user account(s) shall be ended as part of the termination action carried out by the Human Resources Team. Thereafter, the College has the right to access the account for operational reasons and for the continuing delivery of services.

Prior to an employee's termination of contract, line managers should ensure that:

- All IT assets are returned to the College (e.g. laptops, mobile phone devices)

- The employee does 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

No external party shall be given access to any of the College's key systems unless that party has been formally authorised by an appropriate Manager. Prior to access being granted they will be required to sign (electronically or otherwise) the College's ICT Acceptable Use Policy.

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 from the relevant manager.

Key safety procedures to be observed at all times are:

- Staff accounts are rendered inactive when they cease to be employed by the College.

- Learner accounts are rendered inactive and deleted at the end of each academic year.

- Passwords are the responsibility of individual users and must be kept confidential. The passing of an authorised password to someone unauthorised in order to gain access to an information system is a disciplinary offence.

- All systems shall have enforced password change implemented at agreed intervals, all default passwords should be changed on installation.

- The College network perimeter must be protected by a firewall and internet access controlled through a web filtering device. These systems must be tested at regular intervals.

- Anti-virus protection software must be installed on all of the College devices. If a user believes that his/her device is not protected then he/she must contact ICT Support immediately. Users should report any viruses detected/suspected on their equipment to ICT Support immediately.

- All College devices shall be controlled to prevent the installation of malicious or fraudulent software/code.

- The loading and use of unlicensed software on College devices is not allowed.

- Key business systems shall be protected by an additional level of user access control.

- It is the responsibility of the ICT Manager to ensure that access rights and control of traffic on all College networks are correctly maintained. Access rights to core business applications will be controlled by systems managers.

- It is the responsibility of the ICT Manager to ensure that data communications to and from remote networks and computing facilities do not compromise the security of the College ICT systems.

- All hard copy staff, learner, financial, research and corporate records should be stored in a secure area and not left in an unattended, unlocked room. They should only be retained for the minimum length of time that they are absolutely or legally required.

- Access to key IT systems and key data and information assets will only be granted on a need to know basis.

- Data processing security awareness training and/or instruction will be compulsory for all new staff as part of the College's induction process. Refresher training will be delivered annually.

5.4 Access to Personal Data

Subject to limited statutory exceptions, all staff and learners are entitled to know what information the College processes about them and why.

Any person who wishes to exercise their right to view information held about them by the College should make a Subject Access request. Learners should write to the Director of Learner Services, Planning and Diversity and staff should write to the Director of Human Resources with proof of their identity and details of the information they wish to see.

The College will aim to comply with requests for access to personal information within 21 days of receipt of the request and no later than one month from the receipt of the request.

Access will not necessarily be given to the following types of information:

- References given to third parties by the College.
- Management information where disclosure would prejudice the College's business planning.
- Information which would affect ongoing negotiations with the person who requested access.
- Confidential information, disclosure of which would reveal the informant.
- Information which identifies third parties where those third parties have not given consent to disclosure (subject to legal exceptions).

5.5 Physical Security (including personal data stored electronically and in hard copy)

Controls shall be implemented as appropriate to prevent unauthorised access to, interference with, or damage to, the College's key ICT systems and personal data storage facilities. Key systems and networks will be protected by suitable physical, technical, procedural and environmental security controls.

Key physical security procedures to be observed at all times are:

- File servers and storage arrays that hold or process critical and/or sensitive data will be located in physically secured areas. Access to these facilities shall be controlled and restricted to authorised personnel using the TDSI Access Control System. This authorisation is currently granted to ICT Service, Facilities and Directorate.

- Key IT systems shall be protected by UPS and environmental monitoring.

- Key ICT Infrastructure shall be housed in secure, locked racks.

- All ICT infrastructures shall be managed by ICT Support Services and cannot be worked on or accessed without the authorisation of the ICT Manager.

- Personal ICT equipment may only be connected to the college ICT systems over public wireless SSID's. Personal ICT equipment shall not be allowed to participate in domain membership and will only be granted guest access to available services.

- No hard wired connections shall be made to the College ICT Systems without the authorisation of the ICT Manager.

- Users of College ICT facilities are responsible for safeguarding key data and equipment by ensuring that desktop machines are not left logged-on or they are locked when unattended, offices and classrooms are kept locked and that portable equipment is not exposed to opportunistic theft. In addition sensitive or personal data in hard copy format must not be left unattended and should be locked in secure storage when not in use.

- Inactive PCs or terminals shall be set to time out after a pre-set period of inactivity using group policy.

- Users must log off the computer network or initiate a password-protected screensaver when leaving a workstation unattended to prevent anyone else accessing the network using their security credentials. A member of staff or learner that fails to do this will be deemed to be the person accessing the network unless it can be proven otherwise.

- Users of portable equipment belonging to the College 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 College staff to which it is issued and should be secured when not in use. In particular users should take appropriate precautions to prevent snooping and unauthorised viewing of their device screen whilst working at home or in off-site business premises.

- Users must contact the ICT Support if they are aware of, or suspect a security breach.

- Any computer or mobile device that is perceived to be placing the integrity of the College's ICT network at risk will be disconnected.

- An electronic inventory of all IT equipment and software will be maintained. The ICT Manager will have responsibility for inventories on all of the College campus sites.

- IT equipment may not be removed from the College unless it is specifically issued to a user and a Portable Equipment Loan form has been completed and authorised.

- Managers shall follow the Project Approval Procedures which preclude the purchase and commissioning of any ICT equipment, system or software without the approval of ICT Manager.

5.6 Monitoring and Surveillance

The email system is the property of the College and all emails sent and received, including by remote access, may be subject to access and monitoring by the College both during and after users' employment/enrolment at the College. The College may also delete messages or suspend email services to prevent or restrict the flow of messages at its discretion.

All Internet access is monitored and logged for a period of five years. The College may suspend access to the Internet when it is deemed that there is a significant security risk to the College from external sources.

5.7 Remote Access

Specific staff and learners may be granted the capability to access the College's computer network from outside the College's premises. The ability to do so is controlled by ICT Services who must first give express prior consent for remote access. Remote access requires the issuing of secure keys to the user. These keys must not be revealed to anyone or used to remotely connect any other machine/device other than that of the user to whom they are issued. The College reserves the right to terminate remote access and/or to change security keys without prior notification. Remote access to the College's network is monitored by the College in the same way as access made on College's premises.

Staff and learners who are able to access the College's computer network remotely must return to the College any materials, equipment or other items enabling such access upon ceasing their employment or studies at the College.

5.8 Telecommunications

The telecommunications system is the property of the College and any calls made to or from it may be subject to monitoring by examination of the system logs itemised telephone bills.

5.9 Post

Post received at the College's premises is the property of the College. If any post is received which is marked for the attention of individual employees it will generally not be opened prior to distribution. However, the College reserves the right to open and inspect all mail.

Staff and Learners must not use the College as a personal mailing address.

Any mail received by the College for the attention of any learner or member of staff who is no longer a learner or member of staff of the College will be opened and dealt with by the College in whatever manner the College thinks fit.

5.10 CCTV

The Information Commissioner has produced a detailed Code of Practice on the use of CCTV. The Code covers matters such as the size, content and location of warning notices, the positioning of cameras and the handling of tapes.

In accordance with the awarding body requirements, CCTV monitoring may be required during certain exams. All learners and staff present in the exam room will be advised of this requirement prior to the commencement of the exam.

Covert surveillance should not be carried out without the authorisation and active participation of a member of Directorate.

5.11 Storage, Disposal and Transmission

Controls will be implemented as appropriate to ensure that physical devices and electronic media containing college data and information assets (including hard copy) are protected from unauthorised access when in storage, being transmitted or transported and when disposed of.

Key storage, disposal and transmission procedures to be observed at all times are:

- All redundant IT equipment, including Mobile Phones must be disposed according to the appropriate environmental legislation and through an approved contractor. Any storage media (hard disks, SD cards etc.) must be either wiped by the approved disposal contractor and a certificate issued or wiped/physically destroyed by the college using appropriate erasure standards before the media leaves college premises. Equipment and software to achieve this are in the possession of the ICT Services Department.

- Any equipment donated to charity must have all of the storage media wiped using appropriate erasure standards before the media leaves college premises. In addition a document transferring ownership to the charity should be completed by and signed by both the authorised college and charity representatives. The charity must undertake to dispose of any unwanted equipment in accordance with WEEE regulations and indemnify the college from any claims made against them relating to the disposal of the donated equipment.

- Data and information stored on College ICT systems shall not be copied to removable media nor transmitted outside the College without authorisation from the relevant manager.

- Debit/Credit card information must not be stored on College ICT systems, transmitted by email or recorded on paper (with the exception of dedicated card processing machines).

- Data and information classified as restricted that are copied to removable media and/or transmitted outside the College must be encrypted using a recognised standard for encryption such as Microsoft BitLocker.

- Any stolen or misplaced media must be reported to the ICT Manager immediately.

- If a device has ever been used to process personal data then any storage media should be disposed of only after reliable precautions to destroy the data have been taken. Therefore, disposal should only be undertaken by ICT Support who will use an approved disposal contractor.

- Where possible, key data and information assets will be held on a network resource so that it is backed up through a routine managed process. Where this is not possible, provision must be made for regular and frequent backups to be taken.

- Key data and information assets shall not be stored on local hard drives.

- Appropriate on-site and off-site backup procedures must be in place to ensure that data can be restored in accordance with the requirements detailed in the ICT DR Policy.

- The prior approval of the ICT Manager must be sought before using any cloud based services. All users should ensure that the Cloud based service that they are using apply appropriate encryption standards.

6 Data Breaches

- A personal/sensitive personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal/sensitive personal data; e.g. transmission of personal/sensitive personal data to an incorrect email address, disposal of documents containing personal/sensitive personal data in an insecure waste bin, allowing access to a College laptop to an unauthorised user whilst working off site, theft of a College laptop,

- All College staff are responsible for the security of personal/sensitive personal data that they process either electronically or in hard copy version. They are responsible for reporting data breaches immediately to their line manager in accordance with the data breach procedures which are issued separately to this policy. The line manager is responsible for reporting the data breach immediately to the Data Protection Officer (DPO) who will determine if the Information Commissioners Office should be advised of the breach. The DPO only has up to 72 hours since the breach occurred to advise the ICO of a reportable breach.

7 Disciplinary Proceedings

This policy is covered by College disciplinary procedures for staff and learners.