Data Protection Policy

Policy Details			
Policy Owner	Vice Principal; Student and Information Services		
CE Sponsor	Principal & Chief Executive		
Date created this year	07 March 2024		
Version:	**Approved by:**	**Date approved:**	**To be reviewed:**
1	College Executive	12 March 2024	March 2025
1	Audit & Risk Committee	14 March 2024	March 2025

Version Control	
Version Number	**Changes from previous 12 months policy**
1	Updates to job titles throughout the policy, for example to Head of Governance and HR Director
1	Inclusion of Equality Impact Assessment Tool
1	Reference to mandatory three-year refresher for staff
	Changes to policy in year
2	Removal of section ** The conditions listed under Article 9(2) of the GDPR, and replaced with new section 'Individual Rights' Added further comments on data breach log and the use of AI in processing personal data

Equality Impact Assessment Tool

		Yes /No	Comments
1	**Does the policy/guidance affect one group less or more favourably than another on the basis of:**		
	Race or ethnicity	No	
	Disability	No	
	Gender	No	
	Religion or belief	No	
	Sexual orientation	No	
	Age	No	
	Marriage and Civil Partnership	No	
	Maternity and Pregnancy	No	
	Gender Reassignment	No	
2	**Is there any evidence that some groups are affected differently?**	No	
3	**If you have identified potential discrimination, are any exceptions valid, legal and/or justifiable?**	N/A	
4	**Is the impact of the policy/guidance likely to be negative?**	No	
5	**If so, can the impact be avoided?**	N/A	
6	**What alternatives are there to achieving the policy/guidance without the impact?**	N/A	
7	**Can we reduce the impact by taking different action?**	N/A	

Introduction

Colchester Institute needs to retain information about its staff, students and other stakeholders to allow it to carry out its day to day business activities and deliver its strategic objectives, as well as meet legal obligations including data requirements of funding agencies and statutory bodies.

The lawful and correct treatment of personal information is of paramount importance to the organisation and to maintain confidence with all our stakeholders, whoever they are in the wide range of activities we undertake. Through dissemination of this policy we will ensure that the College treats all personal information, including special category data (sensitive personal information) lawfully and correctly.

With the emergence of the General Data Protection Regulation (GDPR), the Government aligned UK law with new EU requirements through the adoption of the Data Protection Act 2018 ('the Act') in May 2018. To comply with the provisions of the Act, the College takes steps to ensure that personal information is collected only where necessary, is stored securely, and is used in accordance with the data protection principles which state that personal data must be – fairly and lawfully processed;

- processed for limited purposes and not in any manner incompatible with those purposes;
- adequate, relevant and not excessive;
- accurate;
- not kept for longer than is necessary;
- processed in accordance with individual's rights;
- held as securely as possible
- not transferred to countries without adequate protection.

Purpose

The purpose of this policy is to ensure that everyone handing personal information is:

- Aware of the Data Protection Act 2018
- Compliant with data protection procedures in all that they do; and
- Ensures that data subjects within their area of management or control are aware of their rights under the Act.

Definitions and interpretation

Scope (information covered by the Act)
'Personal data' covered by the Act is essentially any recorded information (paper and electronic) which identifies a living individual.

Personal Data
To identify an individual, Colchester Institute considers 'Personal data' to be:

 The name of an individual plus any one of the following:

 Date of Birth, Home address, National Insurance Number, Bank Account Details, telephone contact information, next of kin, personal location data (e.g. IP address, cookie identifier, photograph) or any other unique identifier

Special Category Data (previously referred to as Sensitive Personal Data)
As this type of data could create more significant risks to a person's fundamental rights and freedoms, it requires more protection. Generally speaking, in order to process such data there must be a lawful basis in addition to satisfying a condition under article 9 (2) of the GDPR** (See below). The College will generally use explicit consent to process the following special category data:

Any information relating to an individual's *racial or ethnic origin, political opinions, religious beliefs, trade union activities, physical or mental health, physical disabilities, medical, geometric or biometric data, sexual life, sexual orientation*

Whilst details of criminal convictions, care needs, physical disabilities are no longer included under the strict definition (GDPR), for the purposes of Colchester Institute these and any other data of equivalent personal standing, shall be included as 'Special Category Data' and require special protection.

Individual Rights
The College understands its requirements with regard to the Act and supporting individuals rights when it comes to personal data held or processed by the College.

- Individuals have the right to be informed about the collection and use of their personal data. This is a key transparency requirement under the UK GDPR.
- The College will provide individuals with information they are entitled to under the Act when requested, including: the purposes for processing their personal data, the retention periods for that personal data, and who it will be shared with. This is called 'privacy information'.
- The College will provide privacy information to individuals at the time personal data is collected from them.
- If personal data is obtained from other sources, we will provide individuals with privacy information within a reasonable period of obtaining the data and no later than one month.
- We understand that there are a few circumstances when we do not need to provide people with privacy information, such as if an individual already has the information or if it would involve a disproportionate effort or if any request is manifestly excessive.
- The information we provide under a request will be concise, transparent, intelligible, easily accessible, and use clear and plain language.
- We understand there is a need to regularly review, and where necessary, update our privacy information.

Responsibilities
In order to respond to the requirements of the Act, Colchester Institute will:

- fully observe conditions regarding the fair collection and use of information
- meet its legal obligations to specify the purposes for which information is used

- collect and process appropriate information, and only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements
- ensure the quality of the information used e.g. accurate and relevant.
- hold personal information on Management Information Systems for as long as is necessary for the relevant purpose, or as long as is set out in any relevant contract held by the College and in the *Retention of Records Policy* (which defines which records should be kept and for how long).
- ensure that the **rights of people** (see above) about whom information is held can be fully exercised under the Act (these include:
  1. the right to be informed that processing is being undertaken;
  2. the right of access to their personal information;
  3. the right to rectification of information
  4. the right to erasure of information
  5. the right to restrict processing in certain circumstances;
  6. the right to data portability
  7. the right to object
  8. rights in relation to automated decision making and profiling
- take appropriate technical and organisational security measures to safeguard personal information
- ensure that personal information is not transferred without suitable safeguards.
- report any breach or loss of personal data to the Information Commissioner Office (ICO), where it is right to do so and in accordance with prescribed procedures.
- maintain a data breach log and report this frequently to the Corporation Board
- provide appropriate training to staff to ensure they are aware of this policy and their responsibilities in accordance with the Act.
- Not use Artificial Intelligence to process personal data until clear guidelines and procedures are in place

Processes

All personal data will be obtained, as far as possible, from the individual and they will be informed at the time of providing the information, as to how their personal data will be used, in support of the provision of college education and training services and any other related activities.

- Personal data will only be collected for justified reasons and specified purposes. These will normally be communicated, in advance, to the person concerned.
- Personal data processed should be accurate, valid and restricted to that which is necessary to satisfy requirements.
- Special Category Data (Sensitive personal data) may normally only be processed if the person has given their explicit consent. (See page 3)

Important

The security of employee and student data should be comprehensively protected against unauthorised access, improper use, accidental loss, destruction and/or damage, by being kept in locked storage, password protected, or by using other suitable precautions.

Electronic Special Category Data must be password protected and/or encrypted. External hard drives, memory sticks, unencrypted laptops and personal cloud storage must not be used to store sensitive data. Staff must take all precautions necessary to maintain confidentiality of all such information whilst in their possession, whether in soft copy or hard

copy. The IT Security policy must be followed at all times and staff must exercise extreme care when transmitting special category data by email (internally or externally – password protection must always be used).

Personal information should not be disclosed either orally or in writing or accidentally or otherwise to any unauthorised third party. Staff should note that unauthorised disclosure will usually be a disciplinary matter and may be considered gross misconduct in some cases.

Information on authorised access and disclosure for students is included on the College enrolment form. All staff must ensure they confirm any disclosure is authorised and ensure they follow appropriate processes. (Appendix B "Procedure for Police Enquiries/Attendance on Site)

Colchester Institute will ensure:

- all staff are aware of the Data Protection Act and of their required responsibilities.
- all staff are aware of what to do in the event of discovering an actual or suspected breach or loss of information
- everyone managing and handling personal information understands that they are responsible for following good data protection practice
- this policy is available to every member of staff via college portal and changes are communicated as appropriate
    - queries about handling personal information are promptly and courteously dealt with and clear information is available to all staff
    - a Data Protection Officer is appointed
    - all staff receive appropriate training

Obligation of Staff

- staff should be aware of the Act and how the rules apply to them.
- managers must ensure their staff are aware of the rules, and the onus is on them to recognise any data protection risks and tailor training for their staff accordingly.
- staff must complete data protection induction and training, including a three-year refresher course.
- staff have a responsibility to ensure that they respect confidential information in their possession and maintain information security. Unauthorised disclosure of confidential information to a third party, or assisting others in disclosure, will be viewed by Colchester Institute with the utmost seriousness. Staff should ensure extra vigilance when working off site and/or at home.
- staff must assure themselves that any personal data being disclosed is done so for a legitimate business purpose and that the person or agency in receipt of such information is entitled to receive it.
- where authorised to disclose information, staff are responsible for ensuring that all personal data provided supplied is accurate and for notifying any errors or changes as these arise
- staff are responsible for ensuring information is kept no longer than necessary and held in accordance with the retention of records policy.
- staff will ensure measures are taken to lock computers when not in use, and prevent monitors from being viewed by others if used in open access areas where personal data could be viewed.

- information containing personal or special category data not be left out on desks where it can be viewed and cleared from desks at the end of each working day.
- staff will immediately report any breach or suspected breach or loss of personal information as detailed below.
- staff must not use personal cloud storage, external hard drives, memory sticks or any other unencrypted devices (eg laptops) to store or transfer special category data.

Obligation of students

- ensuring personal data provided to the College is accurate and up to date
- notification of any errors or changes as these arise e.g. changes of address

Technical Security

The College has in place appropriate security measures as required by the Act. Information systems are installed with adequate security controls and all employees who use these systems will be properly authorised to use them for college business.

The *IT Security Policy* will be published on the College portal. The College relies on computer servers to store data, and will maintain up-to-date antivirus software and appropriate firewalls. Regular back-ups and robust processes for disabling accounts as people leave are in place. Accounts are controlled via groups to ensure only those that need to know certain information have access to that information. A *Mobile Device Acceptable Use Policy* covers mobile security access control. The wireless access points used at the College all require authentication to be used and cannot be accessed by unauthorised persons. The College ensures all emails are scanned with appropriate software and staff training records are maintained by Human Resources. The College will test the strength of its IT Security Controls from time to time using external expertise and will secure Cyber Essentials Certification annually as a minimum.

Designated Data Controllers

The College has designated Data Controllers with responsibilities for employee and student records as detailed below. Data Controllers determine the purposes for which and the manner in which personal data is processed. They also ensure the sharing of information is undertaken in accordance with this policy.

Director of Human Resources	- employee records
Head of Admissions, Registrations and Exams	- student records
Director of Estates	- CCTV

Breach Reporting

The College is required to notify the ICO in the event of a data security breach. Any staff member who is concerned about data loss must immediately contact the College's nominated Data Protection Officer (DPO). This is Alison Bennett, Head of Governance. Contact details are reproduced below:

Email: dpo@colchester.ac.uk
Tel: 01206 712606

The Data Protection Officer will investigate any concern from the details provided. The person reporting the breach must provide as much information as possible in order for the investigation to take place. The DPO will involve Data Controllers and members of the College Executive as required. The outcome of the investigation will determine whether there will be a requirement to report the breach to the ICO under relevant guidelines.
https://icosearch.ico.org.uk/s/search.html?query=general+data+breaches&collection=ico-meta&profile=_default

Entitlement to Access to Personal Data
Employees and students are entitled to make a formal request to access any personal data which is being used or "processed" by a computerised system and personal information kept about them as part of a "relevant filing system". Requests must be made in writing as stated below. The College aims to comply with requests for access to personal information as quickly as possible and will ensure that it is provided within 40 days of the request.

Employees
Employees wishing to access such personal data must complete the Subject Access Request Form (see appendix A) and submit to the Director of HR (Data Controller – employees).

Students
Students wishing to access such personal data should complete the Subject Access Request form (see Appendix A) which is also available from the Registry Department at the Colchester campus or Information Centre at Braintree. In some cases we may need to ask for proof of identification before the request can be processed

Rights of people (detailed on page 5 under responsibilities)
To ask the organisation to take any of these steps, the individual should send the request to dpo@colchester.ac.uk

Sharing information with parents
The student declaration on the enrolment form includes the statement "I understand that Colchester Institute may contact my parent/guardian regarding my attendance, progress, achievement, wellbeing, welfare and personal safety until the end of the academic year in which I turn 18 years of age", which provides consent for us to share appropriate information, including following up attendance, sending reports home and discussions at parent events.

If a parent/guardian of a student in this age range requests information about their son or daughter than this can be released provided they are named as the next of kin on EBS or ProMonitor and that the member of staff releasing the information has taken steps to ensure the authenticity of the enquirer, and the accuracy of the information given. To eliminate errors as many checks as possible relating to the subject of the inquiry must be made, e.g.

- Full name (not just initials)
- Spelling of name

- Address
- Date of birth
- Course attended
- Next of kin – name and address / phone number

If the staff member is not satisfied that the enquirer is not genuine, or the named next of kin, then they must not release the information.

A student can provide up to date information about their next of kin at Registry or one of the Information Centres.

Students 19 and over
No information can be shared with the parent/guardian of a student aged 19 or over without the express consent of the student.

Third Party requests for student data (including parents not listed as Next of Kin)

Personal Data and Academic References

All requests must be in in writing. The student's permission will be required before the information is released. This will either be by the consent given at enrolment on the enrolment form, or if outside the remit of the criteria on the privacy statement additional written consent from the student will be required before any information is released. All written requests should be sent to:-

Personal Data:- Registry Department, Colchester Institute, Sheepen Road, Colchester, CO3 3LL

Academic References:- Requests should be emailed to academic.references@colchester.ac.uk

Any query regarding the implementation of this procedure or if individual cases occur where a member of staff is uncertain, reference must be made in the first instance to the relevant Data Controller. In no circumstances should students or other enquirers be given private addresses or telephone numbers of staff or other students.

See Appendix A, Procedures for the Release of Student Data for more information, including requests from individuals or agencies

Any other requests for information from external agencies should be referred in the first instance to Registry for action under these procedures.

College Publications
Personal information in the public domain for genuine business purposes, such as names, job titles, etc. included in marketing publications, telephone directory, notice boards, is exempt from the Act. However, any employee or student who

has good reason for wishing to be excluded from such public information should contact the relevant Data Controller.

Use of CCTV

The College's Closed Circuit Television Code of Practice complies with the ICO's CCTV Code of Practice and is the responsibility of the Security Manager. Please refer to the College's *CCTV Code of Practice*

Disposal of Confidential Waste

Employees must ensure that they dispose of all personal and sensitive data securely. E.g. Using the confidential waste bags or shredders. Documentation containing special category data must be kept secure whilst waiting to be confidentially shredded (eg Shredding sacks half-filled must be locked away). No documentation containing sensitive personal data will be placed in waste paper or re-cycling bins.

Other Relevant / Associated Policies Documents:

- *CCTV Code of Practice*
- *IT Security Policy*
- *Mobile Device Acceptable Use Policy*
- *Retention of Records Policy*
- *Staff Disciplinary Policy*

Appendix A

FORM FOR MAKING A SUBJECT ACCESS REQUEST

Name:
Daytime telephone number:
Email:
Address:
Employee Number / Student Number:
By completing this form, you are making a request under the Data Protection Act 2018 for information held about you by the College that you are eligible to receive
Required information (and any relevant dates): [Example: Emails between “A” and “B” from 1 May 2023 to 31 July 2023]
By signing below, you indicate that you are the individual named above. The organisation cannot accept requests regarding your personal data from anyone else, including family members. We may need to contact you for further identifying information before responding to your request. You warrant that you are the individual named and will fully indemnify us for all losses, costs and expenses if you are not. Please return this form to Data Controller Student data subject access request: louise.backhouse@colchester.ac.uk Staff data subject access request: kate.hancock@colchester.ac.uk Please allow up to 1 calendar month for a reply
Data subject’s signature:
Date:

Appendix B

Procedure for Police Enquiries/Attendance on Site

Colchester Institute seeks to support its local police in the conduct of their enquiries. However, it must also ensure its duty of care to both learners and employees and must act in accordance with its duty of confidentiality under Data Protection Law. It is important, therefore, that procedures are followed in the event of a police enquiry made to the College and /or when officers attend on site in the course of their duties.

Requests for Information

All enquiries from police officers for information, whether by telephone or letter or other means should be referred in the first instance to:

1. Vice Principal Student and Information Services - in cases involving learners
2. Director of HR – in cases involving members of staff
3. The Principal or other College Executive member, in the absence of either of the above
4. The Senior Registry Assistant with responsibility for data release

In instances of requests for personal or detailed information about an individual, the request should be accompanied by a completed A101 form confirming the exact information that is required. A record of information on learners disclosed to the Police will be held by the Senior Registry Assistant with responsibility for data release, and no data will be released without the consent of one of the staff listed in 1, 2 or 3 above.

Whilst each case will be judged on the particular circumstances pertaining, the guiding principle should be to comply with reasonable requests for information within the constraints of Data Protection.

Where Safeguarding information is requested from authorised persons (including the Police; Social Services and Local Safeguarding Children Boards (LSCBs) under a Section 47 of the Children Act 1989 enquiry or where there is “reasonable cause to believe that a child or young person may be suffering or at risk of suffering significant harm,” that information will be shared by a member of the Welfare and Safeguarding Team. For vulnerable adults the same procedure applies. A record of what information has been shared and with whom will be maintained in the Safeguarding files.

Police Officers Attending on Site

All enquiries from police officers attending on site should be dealt with in accordance with the following procedure:

- Police officer reports to reception, signs in and waits to be collected.
- Reception contact relevant member of staff, as above

- Police officer is collected and accompanied to an interview room. In no circumstances should police officers be invited to move within the site unaccompanied.
- The relevant senior member of staff will establish the reason for Police attendance and instigate appropriate enquires, or seek to provide the relevant information (with completed A101 as necessary)

Should a police officer reasonably wish to see a particular individual, whether learner or member of staff:

- The relevant senior member of staff will make discreet arrangements for the person concerned to be seen by the Police. Efforts should be made to avoid situations where the person concerned is compromised in their work situation. If the person is a learner of 18 years or younger, they should be accompanied by a member of staff at all times.
- In all cases where a learner is under 18 or is classed as vulnerable either because of learning difficulty or disability, the parent/carer will be contacted immediately. Where the parent/carer cannot be contacted then a member of staff will remain with the learner at all times to provide appropriate advocacy.
- Officers attending will be fully briefed by staff on the nature of any disabilities or learning difficulties and, where appropriate, will be assisted in communicating with the learners.
- A full record of all actions taken will be maintained by the senior member of staff present.
- Once the matter is resolved, the police officer should be accompanied in their return to Reception, where they can sign out and leave the site.
- If deemed necessary, security staff should be requested discreetly to support any of the above processes.

Note: These procedures apply in all instances when the Police themselves instigate an enquiry or visit to the college. In circumstances when the college itself calls upon the police to attend on site (e.g. in response to an emergency), arrangements must be made to ensure that they are met on arrival and taken to the location of the incident or event requiring their presence.

Notification from the Police about a learner or member of staff

If a learner or member of staff is considered by the Police to pose a risk, due to an arrest or previous criminal conviction, they Police will write to either:

1. Vice Principal Student and Information Services - in cases involving learners
2. Director of HR – in cases involving members of staff

- For learners, refer to the Pending Prosecution or Criminal Convictions Policy for Enrolled Students for further action.
- For members of staff, the Director of HR will liaise with the relevant line manager / member of College Management Group to make a decision based on a risk assessment basis. A referral may be made to the Local Area Designated Officer (LADO) if the member of staff may be considered a risk to others, including learners or other staff, the decision whether or not to refer will be made jointly by the Vice Principal Student and Information Services and the Director of HR.

- Records of all cases relating to staff members, including LADO referrals, will be securely retained by the HR Department.