



Data Protection Policy

Reference No MIS 002

Department/Area: MIS

Approved by: Executive Team **on:** September 2017

Issued by: Head of MIS **Responsibility** **Vice Principal, Strategic Partnerships and Professional**

Issue Number: 3 **Number of pages: (including this one)** 17

Next review date: May 2018
(Introduction of GDPR)

The **purpose** of this policy/procedure is to:

- give guidance with respect to data protection principles set out in the Data Protection Act 1998
- work towards compliance with the EU General Data Protection Regulation (GDPR) rules which come into force and will replace the previous Act on 25 May 2018

The **scope** of this policy/procedure is all staff and students.

CENTRAL BEDFORDSHIRE COLLEGE

Data Protection Policy

Introduction

Central Bedfordshire College is committed to protecting the fundamental rights and freedoms of individuals including their right to privacy with respect to the processing of personal data.

Central Bedfordshire College needs to keep certain information about its employees, students and other users to allow it to monitor performance, achievements, and health and safety, for example. It is also necessary to process information so that staff can be recruited and paid, courses organised and legal obligations to funding bodies and government complied with.

To comply with the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. To do this, Central Bedfordshire College must comply with the Data Protection Principles which are set out in the Data Protection Act 1998 (DPA). Additionally, the College is working on the further update and amendment to this policy in advance of the introduction of the EU General Data Protection Regulation (GDPR) that comes into force and replaces the Act on 25 May 2018. The DPA applies to personal data held in any medium (paper, computer database/file, etc). The College recognises its requirements under the DPA, primarily to protect privacy and to avoid causing harm to individuals. This means holding good quality information and keeping information securely in the right hands. In addition to being open and transparent, the College will seek to give individuals as much choice as is possible over what data is held and how it is used.

Personal data is defined as information relating to a living individual who can be identified from the data, or from the data plus other information held (or likely to be held) by the organisation.

There is a subsection of personal data known as sensitive personal data, which includes information regarding racial or ethnic origin, political opinions, religious beliefs, membership of trade unions, physical or mental health, sexual life, the commission or alleged commission of any offence, and any related proceedings. The GDPR will extend this to include philosophical beliefs, genetic and biometric data.

Information we process includes personal details, lifestyle and social circumstances, financial details, student records, vetting checks, etc. It also includes sensitive personal data defined above. We sometimes need to share the personal information we process with the individual concerned and also with other people or organisations.

Full details in respect of the above are provided through the College entry in the Register of Data Controllers, available through the Information Commissioner's Office at <http://ico.org.uk/>. In particular, we are required to make data returns concerning both staff and students to the Education & Skills Funding Agency (ESFA) and the Higher Education Statistics Agency (HESA)

Responsibilities

The DPA regulates how the College can process personal information and we are required to follow eight principles, that personal data should be:

- fairly and lawfully processed
- processed for limited purposes
- adequate, relevant and not excessive
- accurate and where necessary kept up to date
- not be kept longer than necessary
- processed in accordance with the data subject's rights
- secure, with appropriate technical and organisational measures in place against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to personal data
- not be transferred to countries outside of the European Economic Area unless that country ensures an adequate level of protection

The GDPR will expand the first three bullets, requiring personal data to be processed fairly and lawfully and in a transparent manner, that personal data shall be obtained only for specified, explicit and legitimate purposes, and shall be limited to what is necessary.

Central Bedfordshire College and all staff or others who process or use any personal information must ensure that they follow these principles at all times. In order to ensure that this happens, Central Bedfordshire College has developed the Data Protection Policy.

This policy applies to all staff working for, or on behalf of, Central Bedfordshire College and includes direct employees, employees of other organisations working for or in association with the College, associates and contractors or other third parties with legitimate access to College data or systems. Any breach of the data protection policy or the Data Protection Act 1998 (DPA) (the Act) will be automatically considered as a breach of discipline and existing College disciplinary proceedings will apply.

Board of Goverors

The College is the Data Controller as far as the Data Protection and GDPR are concerned and therefore the Board of Governors is ultimately responsible for compliance with data protection legislation. This responsibility is discharged through the Principal and the Senior Leadership Team and onward through the chain of line management in both academic and business support areas.

Vice Principal, Strategic Partnerships and Professional Services

The College has appointed the Vice Principal, Strategic Partnerships and Professional Services as the 'Data Protection Officer' who is responsible for dealing with day-to-day data protection matters and for developing and encouraging good information handling practice amongst all members of the College.

Managers

All staff in managerial or supervisory roles have the responsibility of overseeing compliance and developing good data protection practice within their designated areas, and as part of this should ensure that the staff they supervise understand their responsibilities.

All Staff

Agreement to Central Bedfordshire College processing personal data is a condition of employment for staff. This includes information about previous criminal convictions. The College has a duty under the Children Act and other enactments to ensure that staff are suitable for the job. Central Bedfordshire College also has a duty of care to all staff and students and must therefore make sure that employees and those who use Central Bedfordshire College facilities do not pose a threat or danger to other users. All employees will be DBS checked.

Processing Sensitive Information

Sometimes it is necessary to process information about a person's health, criminal convictions, race and gender and family details. This may be to ensure Central Bedfordshire College is a safe place for everyone, or to operate other Central Bedfordshire College policies, such as the sick pay policy or equal opportunities policy. Because this information is considered sensitive, and it is recognised that the processing of it may cause particular concern or distress to individuals, staff and students will be asked to give express consent for Central Bedfordshire College to do this. More information about this is available from the College's HR Department.

All members of the College are responsible for complying with the Data Protection Act and this policy, and ensuring that any personal data they supply to the College is accurate and up-to-date.

Any member of staff, who considers that the policy has not been followed in respect of personal data about themselves, should raise the matter with the College's data controller.

All staff are responsible for:

- Checking that any information that they provide to Central Bedfordshire College in connection with their employment is accurate and up-to-date.
- Informing Central Bedfordshire College of any changes to information, which they have provided. i.e. changes of address.

- Checking the information that Central Bedfordshire College will send out from time to time, giving details of information kept and processed about staff.
- Informing Central Bedfordshire College of any errors or changes. Central Bedfordshire College cannot be held responsible for any errors unless the staff member has informed Central Bedfordshire College of them.

Security of Personal Data

Members of the College are responsible for ensuring that any personal data they hold are kept securely and not disclosed either orally or in writing, accidentally or otherwise to any unauthorised third party (e.g. papers left on desks).

Best practice should be followed to ensure that personal data for any individual is held only within the allotted College system e.g. student records system, staff records system. Exceptionally for specific and authorised purposes, such data may be located in alternative safe locations, namely College network drives where security control is maintained. It is **NOT** permitted to download personal data to any other format such as hard disk, memory stick, or laptops. You must **NOT** email information to a personal email account or upload to any unsecure platforms.

Staff should note that unauthorised disclosure may lead to disciplinary action being taken.

IT have a separate Policy covering the storage, security and disaster recovery of data.

Students

Students must ensure that all personal data provided to Central Bedfordshire College is accurate and up to date. They must ensure that changes of address, etc. are notified using the "Student Change form" which is available from Reception.. This will enable the College to update its records held in the Management Information System.

Agreement to Central Bedfordshire College processing data collected on a student within the enrolment form or other data provided by the student or others whilst the subject is a student, is subject to a declaration on the College's enrolment form and signed by the student.

Compliance with data protection legislation - processing personal data

Personal data must be processed fairly, lawfully and in a transparent manner and therefore individuals should be made clearly aware of how the College intends to use their personal data.

All students are provided with a privacy notice on their enrolment form when they join the College outlining in general terms how the College uses their personal data.

Staff are made aware through HR induction processes.

In both cases, this information will be developed to ensure compliance with the GDPR.

When processing personal data by/in the College, one of the following conditions must be met:

- The individual has given consent.
- The processing is necessary for the performance of a contract.
- The processing is necessary for a legal obligation.
- The processing is necessary for the protection of the data subject's vital interests.
- The processing is necessary for the exercise of any other functions of a public nature exercised in the public interest.
- The processing is necessary for the purposes of legitimate interests pursued by the data controller.

Additional conditions apply when processing sensitive personal data. As a general rule, the College will only process sensitive data on the basis of explicit consent of data subjects, in order to protect the vital interests of the data subject or another person or where a legal obligation exists. In exceptional circumstances personal data may be disclosed to a third party for the following purposes:

- it is required to safeguard national security
- it is necessary for the prevention or detection of crime
- it is necessary for the discharge of regulatory function including securing the health, safety and welfare of persons at work
- it is to be used for research purposes only
- it is available to the public under law (including Freedom of Information legislation)
- it is necessary to establish, exercise or defend legal rights.
- there is a legal duty to disclose the information

Transfer to Data Processors and Contractors

Any third party or contractor who has access to personal data and/or is acting as a data processor should be fully aware of their obligations to comply with the Data Protection Act and be contracted to act accordingly. Personal data will not be transferred to any country outside of the European Economic Area (EEA).

Personal Information in the Public Domain

It is considered necessary for the College's legitimate interests for certain personal information about its staff to be in the public domain. Personal data classified as being in the 'public domain' refers to information which will be publicly available world-wide and may be disclosed to third parties without recourse to the individual.

The College policy is to make the following items of personal data freely available unless individuals have objected:-

- Names of members of the Board of Governors, Academic Board and Senior Leadership Team
- Names and qualifications of academic and of support staff where appropriate
- Academic staff biographies and curricula vitae
- Staff workplace e-mail addresses and telephone numbers
- Any additional information relating to individuals which they have agreed to be placed in the public domain and which may be in automated and/or manual form.

Any individual who has good reason for not wanting his/her work telephone number or e-mail address to be made public may specify a department telephone number or e-mail address instead.

The College will take all reasonable steps as necessary to ensure that personal data not in the 'public domain' is secure from unauthorised or unlawful processing and accidental loss, damage or destruction, will process the data in accordance with current legislation and the College's Data Protection Register entry and will not disclose the information to any unauthorised third party

Notification of Data Held and Processed

All staff, students and other users are entitled to:

- know what information Central Bedfordshire College holds and processes about them and why.
- know how to gain access to it.
- know how to keep it up to date.
- know what Central Bedfordshire College is doing to comply with its obligations under the 1998 Act.

Rights to Access Information

Staff, students and other users of Central Bedfordshire College have the right to access their personal data held by the College unless a valid exemption exists. Any person who wishes to exercise this right should complete the College's "Request for Access to Data" form (see Appendix 4)

Central Bedfordshire College will make a charge of £25 on each occasion that access is requested, although Central Bedfordshire College has discretion to waive this.

Central Bedfordshire College aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 30 days unless there is good reason for delay. In such cases, the reason for delay will be explained in writing to the person making the request.

Retention and destruction of Data

The College retains data (including Personal Data) in line with differing requirements according to the nature of the record.

Students

In general, information about students will be kept for 7 years after they leave the College.

Staff

Personal data for staff is held by the HR department for 7 years after departure at the end of employment contract, with salient information necessary for any pensions held indefinitely.

Central Bedfordshire College will need to keep some information about staff for longer periods of time. This will include information necessary in respect of pensions, taxation, potential or current disputes or litigation regarding the employment, and information required for job references.

When appropriate, members of the College must ensure that personal data is destroyed confidentially. Where multiple copies exist, all copies must be destroyed and paper records should be shredded or destroyed using the College's approved confidential waste contractor. The disposal of all electronic equipment that has been used for storing personal data is managed by IT. Contracts are in place to provide for the secure destruction of electronic media which include detailed audit trails and validation of destruction notices.

APPENDIX 1 TO THE DATA PROTECTION POLICY

FAQs

What is the Data Protection Act?

The Data Protection Act (DPA) aims to ensure personal privacy, through giving individuals rights with regards to information about themselves and putting responsibilities on organisations that process this information.

What does the DPA mean for the College?

The College renews registration annually with the Information Commissioner's Office (ICO) which oversees the DPA. The DPA regulates how the College can process personal information and we are required to follow 8 principles, that:

- personal data shall be processed fairly and lawfully
- personal data shall be obtained only for one or more specified purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes
- personal data shall be adequate, relevant and not excessive
- personal data shall be accurate and where necessary, kept up to date
- personal data processed for any purpose or purposes shall not be kept for longer than is necessary
- personal data shall be processed in accordance with the rights of data subjects under the Act
- appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data
- personal data shall not be transferred to a country outside the European Economic Area unless that country ensures an adequate level of protection

What is personal data?

Personal data is defined as information relating to a living individual who can be identified from the data, or from the data plus other information held (or likely to be held) by the organisation.

There is a subsection of personal data known as sensitive personal data, which includes information regarding racial or ethnic origin, political opinions, religious beliefs, membership of trade unions, physical or mental health, sexual life, the commission or alleged commission of any offence, and any related proceedings.

How does the DPA affect how the College uses personal data?

In addition to the 8 principles outlined above the DPA specifies conditions that must be met when processing personal data. The list below is not exhaustive but contains most

of those that might be applicable when processing data by/in the College. When processing personal data one of the following conditions must be met:

- The individual has given consent.
- The processing is necessary for the performance of a contract.
- The processing is necessary for a legal obligation.
- The processing is necessary for the protection of the data subject's vital interests.
- The processing is necessary for the exercise of any other functions of a public nature exercised in the public interest.
- The processing is necessary for the purposes of legitimate interests pursued by the data controller.

When processing sensitive personal data there are additional conditions as below, and again at least one of these must be met:

- The individual has given explicit consent.
- The processing is necessary for compliance with legal obligations in connection with employment.
- The processing is necessary to protect the vital interests of the individual or another person where consent cannot be given by or on behalf of the individual, and the College cannot reasonably be expected to obtain consent
- The processing is necessary to protect the vital interests of another person, in a case where consent of the individual has been unreasonably withheld.
- The personal data has been made public as a result of steps deliberately taken by individual.
- The processing is necessary for the purpose of, or in connection with, any legal proceedings or for the purpose of obtaining legal advice.
- The sensitive personal data relates to racial or ethnic origin, and is for the purpose of identifying or reviewing the existence or absence of equality of opportunity, or relates to treatment between people of different racial or ethnic origins with a view to enabling equality of opportunity to be promoted or maintained, and is carried out with appropriate safeguards for the rights and freedoms of individuals.

How does the College tell students about processing their data?

At enrolment, when students register at the College they sign their enrolment form which includes a statement that provides consent to sharing information. The enrolment form also includes a Data Protection statement which outlines the ways in which the College will process student's personal data.

How can I access student information?

The Student data is held securely within College via a secure database and should not be copied on to any mobile device e.g. memory sticks, external hard drives, laptops or emailed to personal email addresses. Paper copies of Student data should not be

removed from the College premises unless for health & safety reasons i.e. emergency contact list taken on a trip.

What happens if the DPA is breached?

The Information Commissioner has the authority to carry out assessments of any organisations against whom complaints have been made and enforce compliance. Breaches can also be tried in court.

The Act provides for separate personal liability for any of the offences in the Act. If a member of staff consents to an offence committed by the College, or that offence is attributable to any neglect on his/her part, that member of staff can be proceeded against and fined accordingly. Additionally, a data subject has the right to sue for compensation if he/she has suffered damage and/or distress as a result of the College's breach of the data protection regulations.

Offences under the act include:

- Processing without notification
- Failure to notify the commissioner of changes to notification register entry
- Failure to comply with an enforcement notice/information notice/special information notice
- Knowingly or recklessly obtaining or disclosing personal data or the information contained in personal data without the consent of the data subject.

What are my rights under the DPA?

The Data Protection Act gives a number of rights to data subjects e.g. students, staff etc.

- You have the right to be informed by the College whether we or someone else on our behalf is processing your personal data and if so, to give you a description of the personal data, the purposes for which we are processing it and the likely recipients and sources of that personal data. You are also entitled to receive a copy of this personal data. All requests for access must be made in writing to the Data Protection Officer. The College will aim to respond promptly to such a request, and certainly within 1 month.
- You are entitled to request, in writing, that the College does not process personal data where such processing is likely to cause substantial damage or substantial distress to you or another person. There are a number of provisos to this right, in particular:-the damage or distress must be "unwarranted"; or the processing cannot be necessary for fulfilling a contract with you, for fulfilling a legal obligation of the College; or for protecting your vital interests.
- You are entitled to request in writing that the College does not process personal data for the purposes of direct marketing.

- You are entitled, by writing, to request that the College ensures that no decision that significantly affects you is based solely on the processing of personal data by automatic means. An example of automated decision taking could be where the decision to reject candidates for interview is made by computer on the basis solely of psychometric testing. Where a decision which significantly affects you is based solely on such automatic processing, the College must notify you that the decision was taken on that basis as soon as reasonably practicable. Note, though, that any human intervention or discretion will mean that the automated decision-taking provisions do not apply.
- If you suffer damage or distress as a result of the College's breach of any of the requirements of the new Act, you may be entitled to compensation.
- You may apply to the Court for an order requiring the College to rectify, block, erase or destroy data relating to you if they are inaccurate. However, initially please simply contact us if you believe information we hold is incorrect.
- You may request that the Information Commissioner assesses whether or not it is likely that any processing of personal data has been or is being carried out by the College in non-compliance with the Act.

How do I make a request to access my personal information held by the College?

All requests must be made in writing to the College Data Protection Controller/Officer at the address below. Once we receive your request we may wish to confirm your identity. In order to locate the correct information within the College, we may need to ask you to provide more information regarding what you require.

Vice Principal, Strategic Partnerships and Professional Services
 Central Bedfordshire College
 Kingsway
 Dunstable
 Beds
 LU5 4HG

We may contact third parties in order to obtain consent to disclose the information. Where consent cannot be obtained or is denied we will consider the reasons and the College's duty of care to both parties as specified in the DPA in order to decide whether or not to disclose the information. All requests will be dealt with within 30 calendar days of receipt of payment. The information will be dispatched to you as soon as the above process is complete.

If you require more information about the Data Protection Act 1998, or are unhappy with the way the College has dealt with your request please contact:

The Information Commissioner Wycliffe House Water Lane Wilmslow Cheshire SK9 5AF
www.ico.org.uk

Data Protection Information for Students Appendix 2

Central Bedfordshire College is registered as a Data Controller with the Information Commissioner's Office as required under the Data Protection Act. The College will only process your personal data in accordance with the College's notification and current Data Protection legislation.

Data Protection Controller

The College Data Protection Controller/Officer is the Vice Principal, Strategic Partnerships and Professional Services

Why and how is my data being processed?.

Examples of how we process your data are outlined below, which are meant to give you a good appreciation rather than an exhaustive list.

Certain personal data will be sent to the Education and Skills Funding Agency (ESFA) and the Higher Education Funding Agency (HEFCE) via the data returns that we have to make, Awarding Body's to enable us to register you for your qualifications and Central Bedfordshire Council in the case of 16-18 year old withdrawing from their courses.

We may confidentially and securely share your personal information with third parties who are contracted to provide IT or data services for the College. Such information will only be used to provide the contracted services, and in accordance with the terms of the agreements with the College.

Contact details (including phone numbers) of completing HE students will be sent to HEFCE for the National Student Survey,

Certain data would be shared with law enforcement partners where we have data sharing agreements in place e.g. Police, Probation service and Local Authorities where any safeguarding concerns may arise.

Should you fall into arrears of payment to the College, we may disclose personal data to a third party (e.g. solicitors, debt recovery agents, Courts) to help pursue and recover the debt.

We collect and hold data about your attendance, your achievements and your engagement with College systems. In addition to the obvious uses of this data we may analyse this information to help support your time as a student. Confidential information identifying you will only be accessible to you as well as academic and/or support staff who have a legitimate reason for needing access.

Medical information or certificates supplied to the College will be kept on your student record throughout your programme of study and may be used in support of assessment processes. Information concerning your physical or mental health may be disclosed within the College or with appropriate professionals or professional services externally so that a proper level of care and facilities may be provided.

International students should be aware that personal information including information about your enrolment, attendance and progress at this establishment may be passed to the Home Office for purposes connected with immigration.

How do I make a request to access my personal information held by the College?

All requests must be made in writing to the College Data Protection Officer at the address below. Once we receive your request we may wish to confirm your identity. In order to locate the correct information within the College, we may need to ask you to provide more information regarding what you require.

Vice Principal, Strategic Partnerships and Professional Services
Central Bedfordshire College
Kingsway
Dunstable
Beds
LU5 4HG

We may contact third parties in order to obtain consent to disclose the information. Where consent cannot be obtained or is denied we will consider the reasons and the College's duty of care to both parties as specified in the DPA in order to decide whether or not to disclose the information. All requests will be dealt with within 30 calendar days of receipt of payment. The information will be dispatched to you as soon as the above process is complete.

You have the right to request that information about you remains confidential. However, this may adversely affect the level of support the College can provide for you. If you have any queries at all regarding the use of your data, or wish to restrict the way we may use your data, please email the Vice Principal, Strategic Partnerships and Professional Services, smortimer@centralbeds.ac.uk. In certain circumstances the College may need to share information about you even if you have asked for it to remain confidential, either to comply with health and safety or ensure safety in an emergency.

Once you have provided your consent to the use of your personal data by the College, you retain the right to opt out of this at any time, and can do this by contacting the Vice Principal, Strategic Partnerships and Professional Services, smortimer@centralbeds.ac.uk.

Reference to Data Protection is included on the enrolment form. A verbal summary outlining the above information is made during face-to-face registration in your first week at the College when you are also made aware that when you sign your enrolment form this provides your consent for us to process information as described above.

Appendix 3 Student Enrolment form declaration

How We Use Your Personal Information

This privacy notice is issued by the Education and Skills Funding Agency (ESFA), on behalf of the Secretary of State for the Department of Education (DfE). It is to inform learners how their personal information will be used by the DfE, the ESFA (an executive agency of the DfE) and any successor bodies to these organisations. For the purposes of relevant data protection legislation, the DfE is the data controller for personal data processed by the ESFA.

Your personal information is used by the DfE to exercise its functions and to meet its statutory responsibilities, including under the Apprenticeships, Skills, Children and Learning Act 2009 and to create and maintain a unique learner number (ULN) and a personal learning record (PLR). Your information will be securely destroyed after it is no longer required for these purposes.

Your information may be shared with third parties for education, training, employment and well-being related purposes, including for research. This will only take place where the law allows it and the sharing is in compliance with data protection legislation.

The English European Social Fund (ESF) Managing Authority (or agents acting on its behalf) may contact you in order for them to carry out research and evaluation to inform the effectiveness of training.

You can agree to be contacted for other purposes by ticking any of the following boxes:

- About courses or learning opportunities.
- For surveys and research.

- By post.
- By phone.
- By e-mail.

Further information about use of and access to your personal data, details of organisations with whom we regularly share data, information about how long we retain your data, and how to change your consent to being contacted, please visit:

<https://www.gov.uk/government/public/esfa-privacy-notice>



Appendix 4 Request for Access to Data Form

To	<input type="text"/>
From	<input type="text"/>
Date	<input type="text"/>
Re: Subject access to personal data	
<p>I understand that the organisation holds personnel records on computer. I am writing to request that you provide a copy of all information that you hold about me to *me/[Enter name] (who is acting as my agent).</p>	
<p>I understand that the information will be provided within 40 days of the above date.</p>	
I enclose a fee of £	<input type="text" value="25:00"/>
Signature	<input type="text"/>
<i>*Delete as appropriate</i>	

Appendix 5 Request for Access to Data Letter

Private and Confidential

[Addressee]
[Address line 1]
[Address line 2]
[Town]
[County]
[POSTCODE]

[Date]

Dear [Enter name]

Subject access request

Thank you for your letter of [Enter date] requesting [Enter details of data requested].

In order to comply with your request, and in accordance with section 7(2)(b) of the Data Protection Act 1998, before we can process your request, I would be obliged if you would provide us with the sum of £25.00.

I confirm that as soon as we are in receipt of cleared funds, the data requested will be supplied to you within 30 days.

Should you have any queries, please do not hesitate to contact me.

Yours sincerely

[Signatory name]
[Job title/Department]