European Union
European
Social Fund

Leicester College

Document No:	**GP002**
Issue No.	**6**
Issue Date:	**2020-01-07 (COVID-19 revision)**
Renewal Date:	**2021-05-08**
Originator:	**Director of Governance and Policy**
Responsibility:	**Director of Governance and Policy**

DATA PROTECTION POLICY

SUMMARY OF THE POLICY – A QUICK GUIDE TO DATA PROTECTION

- **The College is allowed to collect and use data about individuals in order to operate.**
- **It must use and look after the data carefully and not share or use data for reasons other than those for which they were collected.**
- **Individuals have a number of rights concerning their data, including the right to see what information the College holds, and to make sure the data is accurate.**
- **The College will inform individuals why and for what purpose their data is being used.**
- **Although individuals may be asked to give their consent to provide the data, there are circumstances where the College does not need consent to process individuals' data.**
- **Extra care will be taken when the College receives requests – including from people or bodies outside the organisation – for information about individuals. We will not release any information about students without seeking their permission or unless there is a legitimate reason to do so.**
- **All staff have a responsibility to ensure personal data is used appropriately and kept secure. Failure to safeguard data may result in disciplinary action being taken.**

1. INTRODUCTION

1.1. The College needs to keep certain information about employees, students and other users to allow it to monitor, for example, performance, achievements and health and safety. 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.

1.2. To comply with the law, information must be used fairly, stored safely and not disclosed to any other person unlawfully. The College is registered with the Information Commissioners Office (ICO).

1.3. To do this the College must comply with the Data Protection Principles which are set out in the General Data Protection Regulations (GDPR) and UK data protection legislation. In summary these state that personal data shall be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
- Accurate and kept up to date; inaccurate personal data will be erased or rectified without delay
- Not kept for longer than is necessary for the purposes for which the personal data are processed
- Kept secure against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

1.4. The data controller (the College) is responsible for and must be able to demonstrate, compliance with these principles.

1.5. Definitions of what constitutes Personal Data are set out in **Appendix 1.**

1.6. The College and all staff or others who process or use any personal information, including third parties who process data on the College's behalf, must ensure that they follow these principles at all times. In order to ensure that this happens, the College has developed this Data Protection Policy.

1.7. This policy applies to all College activity including ESF contracts.

2. STATUS OF THE POLICY

2.1. This policy does not form part of the formal contract of employment, but it is a condition of employment that employees will abide by the rules and policies made by the College from time to time. Any failure to follow the policy can, therefore, result in disciplinary proceedings.

3. NOTIFICATION OF DATA HELD AND PROCESSED (PRIVACY NOTICES)

3.1. All staff, students and other users are entitled to:

- Know what information the College holds and processes about them and why
- Know how long the data will be kept
- Know how to gain access to it
- What, if any third parties the College may share data with

- Know how to keep it up to date
- Know what the College is doing to comply with its obligations under the GDPR and subsequent legislation.

3.2. The College will, therefore, provide all staff and students and other relevant users with a standard form of notification. This will state all the types of data the College holds and processes about them and the reasons for which it is processed.

3.3. This information (Privacy Notices) will be included in the appropriate documentation such as application and enrolment forms, student support application forms, transport application forms, staff recruitment and appointment documentation, amongst others. This information will also be available on the Data Protection pages of the College's website and its internal intranet. The format for Privacy Notices is included as **Appendix 2**

4. RESPONSIBILITIES OF STAFF

4.1. Staff are responsible for complying with this policy as it relates to their own and other people's data.

4.2. If, and when, as part of their responsibilities, staff collect information about other people (e.g. about students' course work, opinions about ability, references to other academic institutions or details of personal circumstances) they must comply with the guidelines for staff in **Appendix 3**

4.3. Staff should also complete the mandatory staff training on Data Protection when asked to do so. Failure to do so may result in disciplinary action.

4.4. Staff are also responsible for:

- Checking that any information that they provide to the College in connection with their employment is accurate and up to date.
- Informing the College of any changes to information which they have provided, i.e. changes of address.
- Checking the information that the College will send out from time to time, that provides details of information kept and processed about staff members.
- Informing the College of any errors or changes. The College cannot be held responsible for any errors unless the staff member has informed the College of them.

5. DATA SECURITY

5.1. All staff are responsible for ensuring that:

- Any personal data has been collected and is being processed (used) in a fair and lawful manner.
- Any personal data which they hold is kept securely whether in paper or electronic form.
- Personal information is not disclosed either orally or in writing or accidentally or otherwise to any unauthorised third party.

- Personal data processed for one reason is not reused for another unrelated reason without seeking the consent of the individual.
- Data is accurate, up to date and is not kept longer than necessary.
- All personal data is treated with a high degree of sensitivity and disposed of in line with the procedure for disposing of Confidential Waste – see Waste Management Policy (EC015).
- Any breach of data security is reported **immediately** to the Data Protection Officer and using the reporting form **Appendix 4**, also available from the Data Protection SharePoint site. All data breaches will be logged and investigated. The College may need to report a breach to the ICO within 72 hours so immediate reporting is essential.

Paper Storage

5.2. Paper based personal data should be kept in a locked room, filing cabinet, drawer or other appropriate storage device.

Electronic Storage

5.3. The storage or use of any data processed by Leicester College on local hard disk devices such as personal computers or mobile devices must be avoided unless absolutely necessary. The recommended mechanism for using such data is to keep the data on the Leicester College secure data storage servers in Office 365, SharePoint or central College systems.

5.4. All mobile devices containing stored data owned by Leicester College must use an approved Leicester College method to protect data. Mobile devices are defined to include laptops, Tablets, smart phones, and mobile phones.

5.5. All portable storage devices containing stored data owned by Leicester College must use an approved Leicester College method of encryption to protect data. The use of portable storage devices and unencrypted file sharing mechanisms e.g. Dropbox is prohibited in line with the e-Communications Policy (PP80).

5.6. Laptops must employ full disk encryption with approved Leicester College encryption software. No Leicester College data may exist on a laptop in an unencrypted form.

5.7. All mobile phones and tablets must be secured with a PIN code as a minimum. Leicester College will also employ remote wipe technology to remotely disable and delete any data stored on a Tablet, or Smart phone which is reported lost or stolen.

5.8. Use of personal devices for College business is permitted subject to required cyber-security measures, the E-Communications Policy and the Home Working Policy being adhered to.

5.9. The loss or theft of any mobile device or portable storage device containing Leicester College data must be reported **immediately** to the Data Protection Officer and the IT helpdesk.

5.10. Staff should note that unauthorised disclosure of data or a failure to adequately secure data either paper based or electronically will usually be a disciplinary matter and may be considered gross misconduct.

5.11. Further information is set out in the E-Communications Policy (HR015) and Home Working Policy (HR042).

6. STUDENT OBLIGATIONS

6.1. Students must ensure that all personal data provided to the College is accurate and up to date. They must ensure that changes of address, next of kin contact information etc., are notified to the Information Centres or other person as appropriate.

6.2. Students must also ensure that they make use of personal and College equipment in line with the E-Communications Policy (HR015).

7. RIGHTS TO ACCESS INFORMATION/SUBJECT ACCESS REQUESTS

7.1. Staff, students and other users of the College have the right to any personal data that is being kept about them either on computer or in certain files and may make a Subject Access Request (SAR). Any person who wishes to exercise this right is asked to complete the College “Access to Data” form attached as **Appendix 5** and email it to the Data Protection Officer or hand it in to a College Information Centre who will forward it to the Data Protection Officer. However, requests may be made in person or verbally; in these instances further detail which may be helpful will be requested and the request documented on the SAR log.

7.2. SARs may be made directly to the Data Protection Officer or to any member of staff. Any member of staff receiving such a request should pass it **immediately** to the Data Protection Officer who will initiate the data search and respond to the request. All SARs will be logged.

7.3. SARs made on behalf of someone, including those aged under 18 must be made with the consent of the individual if they are over the age of 13. Proof of that consent will be required. Where the College judges that the individual is not able to give consent, for example, students with profound and multiple learning difficulties, the information will be provided to the named individual on the student’s file.

7.4. There is no charge for SARs. However, where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the College may either:

- Charge a reasonable fee taking into account the administrative costs for providing the information or communication or taking the action requested; or
- Refuse to act on the request.

7.5. The College aims to comply with requests for access to personal information without undue delay and within one month of receipt of the request unless there is good reason for delay. In such cases, the reason for delay will be explained in writing to the data subject making the request and the College will agree an extended deadline of up to a further two months.

7.6. The requester will receive a copy of the data held about them in a concise, transparent intelligible and easily accessible form in writing or in electronic form, or in another form requested by the requester. A draft response to a SAR is included as **Appendix 6.**

8. RIGHT TO RECTIFICATION, DELETION OR OBJECTION TO PROCESSING

8.1. All individuals have the right to request that data held about them be rectified, if it is incorrect or deleted in certain circumstances. Individuals also have the right to object to processing of their data.

8.2. Anyone seeking to have their data amended, rectified or deleted, or to request that their data not be processed should complete the Data Amendment/ Deletion form attached as **Appendix 7.**

9. DATA PROTECTION IMPACT ASSESSMENTS

9.1. For all new data collections or systems which involve data processing, a data protection impact assessment (DPIA) will be conducted as part of the Project Initiation Document.

9.2. Guidance and forms to complete DPIAs are included as **Appendix 8.**

10. DATA SHARING AND THIRD PARTY PROCESSING

10.1. Where personal data including special category personal data is shared with third party organisation, this will be covered by a data sharing agreement and/or appropriate wording within contracts.

10.2. Where the College receives requests for personal data from third parties including parents, it will adopt its standard procedures for verifying the identity of the third party and seeking confirmation that sharing of the data would be fair and lawful. **See Appendix 9** for the current procedure. No data will be shared with a third party unless these assurances are received.

11. PUBLICATION OF COLLEGE INFORMATION

11.1. Information that is already in the public domain is exempt from the Data Protection Act. It is the College policy to make as much information public as possible and details of the information readily available can be found in the College's Publication Scheme available on the College website.

12. SUBJECT CONSENT

12.1. In some cases the College can only process personal data with the consent of the individual. If the data is sensitive, express consent must be obtained for some processing. Agreement to the College processing some specified classes of personal data is a condition of acceptance of a student onto any course and a condition of employment for staff. This is also the case for information about previous criminal convictions.

12.2. Some jobs or courses will bring the applicants into contact with children, including young people between the ages of 14 and 18. The College has a duty under the Children Act and other enactments to ensure that staff are suitable for the job and students for the courses offered. The College also has a duty of care to all staff and students and must, therefore, make sure that employees and those who use the College facilities do not pose a threat or danger to other users.

12.3. The College will also ask for information about particular health needs, such as allergies to particular forms of medication, or any conditions such as asthma or diabetes. The College may also ask for information relating to COVID-19 during the pandemic. The College will only use the information in the protection of the health and safety of the individual, public health reasons or another legal reason.

12.4. In instances where consent is given as the primary fair processing condition, individuals may choose to withdraw their consent. Requests must be submitted in writing using the consent withdrawal form at **Appendix 10.** However where the College has other lawful reasons for processing personal data, it will continue to do so.

13. PROCESSING SENSITIVE/SPECIAL CATEGORY INFORMATION

13.1. Sometimes it is necessary to process information about a person's health, criminal convictions, race and gender, sexual life or political views or beliefs. This may be to ensure the College is a safe place for everyone, or to operate other 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 the College to do this. Offers of employment or course places may be withdrawn if an individual refuses to consent to this, without good reason. More information about this is available from the Data Protection Officer.

14. THE DATA PROTECTION OFFICER AND THE DESIGNATED DATA CONTROLLER(S)

14.1. The College as a body corporate is the Data Controller under the Act and the Board is, therefore, ultimately responsible for implementation. However, there are designated data controllers dealing with day to day matters. The first point of contact for enquirers is

Louise Hazel	Director of Governance and Policy (Data Protection Officer) Freemen's Park Campus, Welford Road, Leicester LE2 7LW
Tel:	0116 224 2023
E-mail:	dpo@leicestercollege.ac.uk

15. EXAMINATION MARKS

15.1. Students will be entitled to information about their marks for both coursework and examinations. However, this may take longer than other information to provide as some information is subject to release by awarding bodies. The College may withhold certificates, accreditation or references in the event that the full course fees have not been paid, or all books and equipment have not been returned to the College.

16. RETENTION AND DISPOSAL OF DATA

16.1. The College will keep some forms of information for longer than others in line with the Records Retention Guidelines (EC011). Because of storage problems, information about students cannot be kept indefinitely, unless there are specific requests to do so. **Appendix 11** provides a summary of the archiving guidelines and retention times employed by the College.

16.2. When disposing of any document containing personal data, care should be taken to ensure that the document is shredded before consigning to the waste collection. Further information is given in the Waste Management Policy (EC015). Where there are bulk quantities of such documents, arrangements should be made with the College's Estates Department.

17. COMPLAINTS PROCESS

17.1. Any complaints concerning the College's processing of personal data should be addressed to the Data Protection Officer in the first instance who will investigate the complaint and make a response.

17.2. In the event that a response has been made and the complainant feels that the complaint has not been properly address, complainants may contact the Information Commissioner's Office. You can contact them on 01625 545745 or 0303 123 1113.

18. CONCLUSION

18.1. Compliance with the Data Protection Act is the responsibility of all members of the College. Any deliberate breach of the Data Protection Policy may lead to disciplinary action being taken, or access to College facilities being withdrawn, or even prosecution. Any questions or concerns about the interpretation or operation of this policy should be taken up with the designated College Data Protection Officer.

15. APPENDICES

1. Definition of personal data/special category data
2. Standard format for privacy notices
3. Staff Guidelines for Data Protection
4. Breach reporting form
5. Standard request for Access to Data
6. Draft response to a SAR
7. Data amendment/deletion request form
8. Data Protection Impact Assessment (DPIA) Guidance and Forms
9. Identity verification process
10. Consent withdrawal form
11. Archiving and retention guidelines (summary)

APPENDIX 1

PERSONAL DATA/SPECIAL CATEGORY DATA DEFINITIONS

Under the GDPR, the data protection principles set out the main responsibilities for organisations.

Article 5 of the GDPR requires that personal data shall be:

“a) processed lawfully, fairly and in a transparent manner in relation to individuals;

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.”

Personal data

The GDPR applies to ‘personal data’ meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.

This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people.

The GDPR applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria. This could include chronologically ordered sets of manual records containing personal data.

Personal data that has been pseudonymised – e.g. key-coded – can fall within the scope of the GDPR depending on how difficult it is to attribute the pseudonym to a particular individual.

Special Category Data

- race
- ethnic origin
- politics
- religion
- trade union membership
- genetics
- biometrics (where used for ID purposes)
- health
- sex life; or
- sexual orientation.

Personal data relating to criminal convictions and offences are not included, but similar extra safeguards apply to its processing.

More information is available from the ICO: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/

APPENDIX 2

STANDARD FORMAT FOR PRIVACY NOTICE

WHAT INFORMATION DO WE HOLD ABOUT YOU?

Information we collect from you

You provide us with personal data when [specify when and how data is collected]. This includes [specify – could include your name, address, date of birth, contact information, gender, next of kin/parent/carers for under 18s and under 25s students with learning difficulties and disabilities, previous education and qualifications, any medical or support needs, bank account information]. We also collect information about ethnicity, medical conditions and offences.

Other information

We also hold other information about you including [specify].

We may keep information contained in any correspondence by post or email. We may record phone calls.

We may also obtain other information about you permitted by law. This may include from previous educational institutions, social services, the police or other agencies. [Specify any other]

WHY DO WE COLLECT THIS INFORMATION?

We collect information in order to enable us to fulfil our legal obligations in relation to providing further education in line with the Further and Higher Education Act 1992, to comply with the requirements of government funding agencies, and to meet other statutory requirements. [specify other lawful reasons].

WHO MIGHT WE SHARE YOUR INFORMATION WITH?

We will keep this information about you confidential. We will share the information with government funding agencies (the Education and Skills Funding Agency, the Office for Students, the Student Loan Company) in order to comply with our legal duties. We may also share the information with national bodies for the purposes of monitoring and research.

We may be asked to share data with other third parties where there is a lawful reason for their request. These may include: the police, social services, legal firms acting on your or the College's behalf, debt collection companies, insurance companies acting on your or the College's behalf, HMRC, other government agencies.

We will not share your details with any other third party including commercial companies without your consent to do so.

[Add any further third parties with whom data will be shared]

WHAT DO WE DO WITH YOUR INFORMATION?

We collect this information in order to [specify].

The information is held on College data management systems and may be used by teaching and support staff in order to support education and training, to report on overall College performance and to safeguard you and other students, staff and visitors.

[Specify other uses – may include the following:
We will use the information to analyse and report, in line with Government requirements, on the College's overall performance against several indicators. As aggregated data it will be used to support the College's claims for government funding and as aggregated and anonymised it will be used by the Department for Education and its agencies to calculate and publish performance data about the College.]

Transfer of your personal data outside of the European Economic Area (EEA)

We do not transfer your personal data outside the EEA.

HOW LONG DO WE KEEP THIS INFORMATION ABOUT YOU?

We keep information in accordance with our records retention policy. Retention periods are in line with the length of time we need to keep your personal information in order to manage and administer your education and training and handle any future information issues. They also take into account our need to meet any legal, statutory and regulatory obligations. These reasons can vary from one piece of information to the next. In all cases our need to use your personal information will be reassessed on a regular basis and information which is no longer required will be disposed of.

HOW CAN I ACCESS THE INFORMATION YOU HOLD ABOUT ME?

Subject access requests

The General Data Protection Regulation (GDPR) grants you the right to access particular personal data that we hold about you. This is referred to as a subject access request. We will respond within one month from the point of receiving the request and all necessary information from you. Our formal response will include details of the personal data we hold about you, including the following:

- Sources from which we acquired the information
- The purposes for processing the information, and
- Persons or entities with whom we are sharing the information.

You can make a subject access request by completing the request form or by emailing it to dpo@leicestercollege.ac.uk.

WHAT ARE MY RIGHTS?

Subject access requests

The General Data Protection Regulation (GDPR) grants you the right to access particular personal data that we hold about you.

Right to rectification

You have the right to obtain from us, without undue delay, the rectification of inaccurate personal data we hold concerning you. Taking into account the purposes of the processing, you have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

Right to erasure

You have the right to obtain from us the erasure of personal data concerning you without undue delay.

Right to restriction of processing

Subject to exemptions, you have the right to obtain from us restriction of processing where one of the following applies:

- The accuracy of the personal data is contested by you and is restricted until the accuracy of the data has been verified;
- The processing is unlawful and you oppose the erasure of the personal data and instead request the restriction in its use;
- We no longer need the personal data for the purposes of processing, but it is required by you for the establishment, exercise or defence of legal claims;
- You have objected to processing of your personal data pending the verification of whether there are legitimate grounds for us to override these objections.

Notification obligation regarding rectification or erasure of personal data or restriction of processing

We shall communicate any rectification or erasure of personal data or restriction of processing as described above to each recipient to whom the personal data has been disclosed, unless this proves impossible or involves disproportionate effort. We shall provide you with information about those recipients if you request it.

Right to data portability

You have the right to receive your personal data, which you have provided to us, in a structured, commonly used and machine-readable format and have the right to transmit this data to another controller, without hindrance from us.

Right to object

You have the right to object, on grounds relating to your particular situation, at any time to the processing of personal data concerning you, including any personal profiling; unless this relates to processing that is necessary for the performance of a task carried out in the public interest or an exercise of official authority vested in us.

We shall no longer process the personal data unless we can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of you or for the establishment exercise or defence of legal claims.

Right to not be subject to decisions based solely on automated processing

We do not carry out any automated processing leading to an automated decision based on your personal data.

Accuracy of information

In order to provide the highest level of customer service possible, we need to keep accurate personal data about you. We take reasonable steps to ensure that accuracy of any personal data or sensitive information we obtain. We ensure that the source of any personal data or sensitive information is clear and we carefully consider any challenges to the accuracy of the information We also consider when it is necessary to update the information, such as name or address changes and you can help us by informing us of these changes when they occur.

WHO CAN I CONTACT IF I HAVE ANY QUESTIONS OR CONCERNS?

If you have any questions or queries which are not answered by this Privacy Notice, or a have any potential concerns about how we may use the personal data we hold, please write to the Data Protection Officer at Leicester College, Freemen's Park Campus, Welford Road, Leicester, LE2 7LW or email dpo@leicestercollege.ac.uk.

If your complaint is not resolved to your satisfaction and you wish to make a formal complaint to the Information Commissioner's Office (ICO), you can contact them on 01625 545745 or 0303 123 1113. You also have the right to judicial remedy against a legally binding decision of the ICO where you consider that your rights under this regulation have been infringed as a result of the processing of your personal data. You have the right to appoint a third party to lodge the complaint on your behalf and exercise your right to seek compensation

PRIVACY NOTICE CHANGES

This Privacy Notice is regularly reviewed. This is to make sure that we continue to meet the highest standards and to protect your privacy. We reserve the right at all times, to update, modify or amend this Notice. We suggest that you review this Privacy Notice from time to time to ensure you are aware of any changes we may have made, however, we will not significantly change how we use information you have already given to us without your prior agreement. The latest version of this Notice can be found at on the College's website.

[date]

STAFF GUIDELINES FOR DATA PROTECTION

1. All staff will process data about students on a regular basis when marking registers or College work, writing reports or references or as part of a pastoral or academic supervisory role. The College will ensure, through registration procedures, that all students are notified of the categories of processing, as required by the law. The information that staff deal with on a day-to-day basis will be 'standard' and will cover categories such as:

    - general personal details such as name and address;
    - details about class attendance, course work marks and grades and associated comments;
    - notes of personal supervision, including matters about behaviour discipline.

Sensitive/Special Category Data

2. Information about a student's physical or mental health; sexual life; political or religious views; trade union membership or ethnicity or race is sensitive; this may only be processed with the student's consent or on the advice and approval of the Data Protection Officer. If staff need to record this information they should seek advice before processing the data.

3. All staff have a duty to make sure that they comply with the data protection principles, which are set out in the College Data Protection Policy. In particular, staff must ensure that records are:

    - accurate
    - up-to-date
    - fair
    - kept and disposed of safely and securely and in accordance with the College policy.

4. Staff should complete the mandatory training when requested to do so and follow the Do's and Don'ts as a further guide to good practice.

5. Staff shall not disclose personal data to any other staff member, except with the authorisation in line with College policy or the agreement of the Data Protection Officer.

6. Before processing any personal data, all staff should consider the checklist.

Staff Checklist for Recording Data

- Do you really need to record the information?

- Is the information 'standard' or is it 'sensitive'/'special category'.

- If it is ‘sensitive’/’special category’, do you have the data subject’s express consent?
- Has the student been told that this type of data will be processed?
- Are you authorised to collect/store/process the data?
- If yes, have you checked with the data subject that the data is accurate?
- Are you sure that the data is secure?
- If you do not have the data subject’s consent to process, have you sought advice that there is a legal reason to process the data?

The Data Protection Office should be advised of any new collections of sensitive/special category data prior to the data processing starting.

APPENDIX 4

DATA BREACH REPORTING FORM

Please complete all sections electronically and return to
dpo@leicestercollege.ac.uk

Name: (person reporting the breach)	
Date of Breach:	
Time of Breach: *The College may need to report a breach to the ICO within 72 hours so immediate reporting and a log of the time is essential.*	
Date reported to data protection officer:	
Reasons for delay in reporting (if relevant):	
Description of breach:	
What type of data has been lost/damaged/destroyed?	
Who (individual/individuals) will be affected by the breach?	
What action has been taken since becoming aware of the breach?	
What action is required to prevent this happening again?	
Any Other Information	

APPENDIX 5

STANDARD REQUEST FORM FOR ACCESS TO DATA

I …… (insert name)

wish to have access to:

Either

1. All the data that the College currently has about me, either as part of an automated system or manual filing system ☐

Or

2. Data that the College has about me in the following categories:

(a)	Academic marks or course work details	☐
(b)	Academic or employment references	☐
(c)	Employment file (staff)	☐
(d)	Disciplinary records	☐
(e)	Health and medical matters	☐
(f)	Political, religious or trade union information	☐
(g)	Any statements of opinion about my abilities or performance	☐
(h)	Personal details including name, address, date of birth etc.	☐
(i)	Other information (please list below)	☐

……

……

……

……

I would like the information provided:

In hard copy ☐

In electronic format (by email) ☐

In another format – please specify……... ☐

Please tick appropriate boxes

I understand that a 'reasonable fee' may be made if a request is manifestly unfounded or excessive, particularly if it is repetitive.

I understand that the College may also charge a reasonable fee to comply with requests for further copies of the same information.

Signed: ……

Date: ……

Please return this form to the Data Protection Officer – dpo@leicestercollege.ac.uk
Or Leicester College, Welford Road, Leicester, LE2 7LW

RESPONSE TO SUBJECT ACCESS REQUEST

TO BE SENT BY EMAIL OR HARD COPY DEPENDING ON HOW THE REQUEST AS HAS BEEN MADE AND THE WISHES OF THE SUBJECT

Date:
Reference:
[address]

Dear [ ]

In response to your subject access request for data held by Leicester College about you, I can confirm the College holds the following data and for the purposes described below.

What data we hold about you and a description of the personal data

[ ]

Why we process the data

[ ]

Whether we share the data with any third parties

[ ]

The source of the data

[ ]

How long we will retain the data

[ ]

Attached/enclosed is a copy of the data.

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

Yours sincerely

Data Protection Officer

APPENDIX 7

REQUEST FOR DATA AMENDMENT/DELETION/END TO PROCESSING

Name	
Address	
Email	
Telephone number	
Student/staff number (if known/applicable)	

Please enter a description of the data which you wish to have amended/deleted/no longer processed:

Please explain why you wish the data to be amended/deleted or why processing should stop.

Signed: ……

Date: ……

Please return this form to the Data Protection Officer – dpo@leicestercollege.ac.uk
Or Leicester College, Welford Road, Leicester, LE2 7LW

DATA PROTECTION IMPACT ASSESSMENTS – GUIDANCE

INTRODUCTION

1. This document provides guidance and templates for conducting Data Protection Impact Assessments (DPIAs).

ABOUT DATA PROTECTION IMPACT ASSESSMENTS (DPIAS).

2. A Data Protection Impact Assessment (DPIA) is a process to analyse data processing and help identify and minimise data protection risks. It must:
   - describe the processing and purposes;
   - assess necessity and proportionality;
   - identify and assess risks to individuals; and
   - identify any measures to mitigate those risks and protect the data.

3. It is a legal requirement that a DPIA should be undertaken before carrying out processing likely to result in high risk to individuals' interests. It does not have to eradicate the risk, but should help to minimise risks and consider whether or not they are justified.

4. DPIAs should consider compliance risks, but also broader risks to the rights and freedoms of individuals, including the potential for any significant social or economic disadvantage. The focus is on the potential for harm, whether physical, material or non-material, to individuals or to society at large.

5. More information is available from the Data Protection Officer or from the Information Commissioner's Office (ICO) website.

WHY AND WHEN TO COMPLETE DPIAS

6. The College must conduct a DPIA before it begins any type of processing which is 'likely to result in a high risk'. This means that although the actual level of risk has not been assessed yet, we need to screen for factors which point to the potential for a widespread or serious impact on individuals.

7. In particular, organisations must do a DPIA if they plan to:
   - use systematic and extensive profiling with significant effects
   - process special category or criminal offence data on a large scale; or
   - systematically monitor publicly accessible places on a large scale.

8. The ICO also requires a DPIA if it is planned to:
   - use new technologies
   - use profiling or special category data to decide on access to services
   - profile individuals on a large scale
   - process biometric data
   - process genetic data
   - match data or combine datasets from different sources;

- collect personal data from a source other than the individual without providing them with a privacy notice ('invisible processing')
- track individuals' location or behaviour
- profile children or target services at them; or
- process data that might endanger the individual's physical health or safety in the event of a security breach.

9. The ICO advises that organisations should also think carefully about doing a DPIA for any other processing which is large scale, involves profiling or monitoring, decides on access to services or opportunities, or involves sensitive data or vulnerable individuals.

10. Even if there is no specific indication of likely high risk, the ICO says it is good practice to do a DPIA for any major new project involving the use of personal data.

GUIDANCE ON COMPLETING A DPIA

11. This guidance has two sections:

    1 **Screening questions** – to help you decide if DPIA is necessary

    2 **Privacy Impact Assessment Form** – the form to complete the DPIA

12. Please work through both sections of this guidance.

13. At each stage of the process, please contact the College's Data Protection Officer to discuss the outcome and agree the next steps.

SECTION 1
DATA PROTECTION IMPACT ASSESSMENT SCREENING QUESTIONS

These questions are intended to help you decide whether a DPIA is necessary.

Answering 'yes' to any of these questions is an indication that a DPIA would be a useful exercise. You can expand on your answers as the project develops if you need to.

	Yes	No
1. Will the project involve the collection of new information about individuals?		
2. Will the project compel individuals to provide information about themselves?		
3. Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?		
4. Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?		
Will the proposed data processing:		
5. Use systematic and extensive profiling or automated decision making to make significant decisions about people.		
6. Process special category data or criminal offence data on a large scale.		
7. Systematically monitor a publicly accessible place on a large scale		
8. Use new technologies.		
9. Use profiling, automated decision-making or special category data to help make decisions on someone's access to a service, opportunity or benefit.		
10. Carry out profiling on a large scale.		
11. Process biometric or genetic data.		
12. Combine, compare or match data from multiple sources.		

	Yes	No
13. Process personal data without providing a privacy notice directly to the individual.		
14. Process personal data in a way which involves tracking individuals' online or offline location or behaviour.		
15. Process children's personal data for profiling or automated decision-making or for marketing purposes, or offer online services directly to them.		
16. Process personal data which could result in a risk of physical harm in the event of a security breach.		
Does the proposed data processing involve any other:		
17. Evaluation or scoring.		
18. Automated decision-making with significant effects.		
19. Systematic monitoring.		
20. Processing of sensitive (special category) data or data of a highly personal nature.		
21. Processing on a large scale.		
22. Processing of data concerning vulnerable data subjects.		
23. Innovative technological or organisational solutions.		
24. Processing involving preventing data subjects from exercising a right or using a service or contract.		

If you have answered 'yes' to any of these questions you will need to conduct a DPIA (Section 2).

Please contact the Data Protection Officer for more information.

SECTION 2
DATA PROTECTION IMPACT ASSESSMENT (DPIA) TEMPLATE

This provides a template for recording the DPIA process and results. You can start to fill in details from the beginning of the project, after the screening questions have identified the need for a DPIA. The template follows the process that is used in the Information Commissioner's Office code of practice.

Step 1: Identify the need for a DPIA **Explain broadly what the project aims to achieve and what type of processing it involves.** You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.

Step 2: Describe the processing **Describe the nature of the processing:** how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or another way of describing data flows. What types of processing identified as likely high risk are involved?
Describe the scope of the processing: what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?
Describe the context of the processing: what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?

Describe the purposes of the processing: what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing for you, and more broadly?

Step 3: Consultation requirements **Consider how to consult with relevant stakeholders:** describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?

Step 4: Assess necessity and proportionality **Describe compliance and proportionality measures, in particular:** what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?

Step 5: Identify and assess risks

Describe the source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	Likelihood of harm *Remote, possible or probable*	Severity of harm *Minimal, significant or severe*	Overall risk *Low, medium or high*

Step 6: Identify measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5

Risk	**Options to reduce or eliminate risk**	**Effect on risk** *Eliminated, reduced or accepted*	**Residual risk** *Low, medium or high*	**Measure approved** *Yes/no*

Step 7: Sign off and record outcomes

Item	**Name/date**	**Notes**
Measures approved by:		*Integrate actions back into project plan, with date and responsibility for completion*
Residual risks approved by:		*If accepting any residual high risk, consult the ICO before going ahead*
DPO advice provided:		*DPO should advise on compliance, step 6 measures and whether processing can proceed*
Summary of DPO advice		
DPO advice accepted or overruled by:		*If overruled, you must explain your reasons*
Comments:		
Consultation responses reviewed by:		
Comments:		*If your decision departs from individuals' views, you must explain your reasons*
This DPIA will be kept under review by:		*The DPO should also review ongoing compliance with DPIA*

DATA DISCLOSURE AND IDENTITY VERIFICATION

Learning, attendance, progress and behaviour/disciplinary

Under 18s	Learning, attendance and progress information **will** be shared with parents/carers of students aged under 18 with the student's consent (collected at enrolment). Information on course withdrawals and exclusions will also be shared with parents/carers.
18+	Learning, attendance and progress information **will** be shared with parents/carers of students aged 18+ until the end of their programme if: • they started the programme *before* the age of 18 • the student consents to this. Learning, attendance and progress information will **not** be shared with parents/carers of students aged 18+ who started their programme *after* the age of 18 without the explicit consent of the student. This must be received in writing.
SEND	Learning, attendance, progress and behaviour information for students with learning difficulties and/or disabilities (within the Supported Learning Area) or students with Education, Health and Care Plans (EHCPs) will be shared with parents/carers for the length of student's programme.

Other Data

Other data will not be shared with parents/carers under normal circumstances unless there are lawful reasons to do so (e.g. safeguarding concerns).

Disclosure to Third Parties

Personal data about students and staff may be disclosed to other third parties without the consent of the individual where there is a lawful reason to do so. This might include disclosures to the Police and Social Services.

For all requests, verification of identity will be required as follows: DATA SHARING/IDENTITY VERIFICATION		
ENQUIRY RECEIVED FROM		
Parent/carer	**Police**	**Social Services/Other Agency**
Confirm identity by asking the following questions	**Confirm identity by asking the following questions**	**Confirm identity by asking the following questions**
• Confirm student's DOB • Check the age of the student (18+ we will not discuss without the student's consent) • Name • Address • Relationship to the student • What course is the student doing? • Who should we have on record as the next of kin? • What mobile number(s) should we have for either the student or the next of kin? Customer Service Centres: request over the phone Student Services: request in writing	• Ask for full name of the person calling and address of the police station he is stationed at • Ask for collar number • Ask for telephone number • Confirm the caller is a police officer, either by ringing 0116 2222222 (Leicestershire Police, Police Constable) • Give our direct telephone number and name of contact here.	• Ask for full name of the person calling and location of their centre • Ask for telephone number • Ask for the request to be made in writing using an official form or where there is no official form to use then an email from the individual from their work email address should be requested. • Alternatively call the professional back via their switchboard to check they are who they say they are. • Give our direct telephone number and name of contact here.
Next Steps	**Next Steps**	**Next Steps**
• If the ID is confirmed, provide the requested data or refer on as appropriate • If the caller cannot give us a correct answer for these questions, a valid reason for calling, you have doubts about the caller or if there is no consent from the student, **refuse** to give out any information.	• Check that the student is enrolled at the College. • You can then contact the Police to confirm this, but no further information should be given • Any information requires a Data Protection Form to be completed. • If the student is under 18, pass the enquiry to the Safeguarding Team and inform the Police of this	• Check that the student is enrolled at the College. • You can then contact the individual requesting to confirm this, but no further information should be given • Any information requires a Data Protection Form to be completed. • If the student is under 18, pass the enquiry to the Safeguarding Team and inform the requestor of this
Things to remember	**Things to remember**	**Things to remember**
• Parents do not have an automatic right to information about their child, regardless of their age. • Check EBS for any comments about parental/carer contact.	• Police cannot enter the College without ID or the required Data Protection form if they require information.	• The College has a duty to safeguard students. This may permit the disclosure of data – if you are not sure, seek advice.

APPENDIX 10

WITHDRAWAL OF CONSENT FORM

I …… (insert name) wish to withdraw my consent to the processing of data that the College has about me in the following categories:

(a)	Personal details including name, address, date of birth etc.	☐
(b)	Race, religion, ethnic origin	☐
(c)	Health and medical matters	☐
(c)	Sexual life	☐
(d)	Political, religious or trade union information	☐
(e)	Criminal offences	☐
(f)	Use of photographs for promotional purposes	☐
(g)	Use of other personal data for promotional purposes	☐
(h)	Use of personal data for research purposes	☐
(i)	Other information (please list below)	☐

……

……

……

……

Signature……..

Date…….

Please note that the College may not require consent for the processing of some data in order that it continues to fulfil other statutory obligations. Withdrawal of consent may therefore not affect the College's ability to process your data.

Please return this form to the Data Protection Officer – dpo@leicestercollege.ac.uk
Or Leicester College, Welford Road, Leicester, LE2 7LW

APPENDIX 11

ARCHIVING AND RETENTION GUIDELINES

Type of Data	Retention Period	Reason
Personnel Files; training records; notes of grievance and disciplinary hearings	6 years from the end of employment	Provision of references and limitation period for litigation
Staff Application forms; interview notes	6 months from the date of the interviews	Limitation period for litigation
Facts relating to redundancies (less than 20)	3 years from the date of redundancies	Limitation period for litigation
Facts relating to redundancies (20 or more)	12 years from the date of redundancies	Limitation period for litigation
Income Tax and NI returns; correspondence with Tax Office	3 years after the end of the financial year to which the records relate	Income Tax (Employment) Regulations 1993
Statutory Maternity Pay records and calculations	3 years after the end of the financial year to which the records relate	Statutory Maternity Pay (General) Regulations 1986
Statutory Sick Pay records and calculations	3 years after the end of the financial year to which the records relate	Statutory Sick Pay (General) Regulations 1982
Wages and salary records	6 years from the last date of employment	Taxes Management Act 1970
Records and reports of accidents	3 years after the date of the last entry	RIDDOR 1985
Health Records	During Employment	Management of Health and Safety at Work Regulations
Health Records where reason for termination of employment is concerned with health, including stress-related illness	3 years	Limitation period for personal injury claims
Medical Records kept by reason of the Control of Substances hazardous to health	40 years	COSHHR 1994
Student Records including academic achievements and conduct	6 years from the last day of the course. 10 years with the consent of the student for personal and academic references	Limitation period for negligence
Records relating to funds administered under the European Social Fund	31 December 2030 at the earliest	ESF Guidance