# Student Education Data Protection Training

Authored by Alice Temple Data Protection Officer, Neil Favager IT Assurance Manager and Helen Billington GDPR Manager for SES. January 2021

## Aims

* Increase knowledge and understanding of University’s requirements for GDPR compliance
* Provide guidance on key issues that can arise and how to address them.

## Overview

* We will cover the lawful basis for data processing
* Consent – information to include
* Data Protection Impact Assessments – when these are needed
* How to handle personal data
* Data Sharing
* Data Breach Reporting

## Personal Data

What is it?

Data whereby an individual can be identified or who are identifiable, directly from the information in question; or who can be indirectly identified from that information in combination with other information – Information Commissioner’s Office

This includes names, e-mail addresses, postal addresses, identification numbers, location data and online identifiers such as IP addresses and cookie identifiers.

## Pseudonymised Data

Pseudonymised data is data that has had the identifiers removed. Pseudonymised data reduces the privacy risk as it is harder to identify individuals, but it is still personal data.

If the data is anonymised, it is no longer personal data so we need to understand what personal data is in order to understand if it has been anonymised properly.

## GDPR 7 Principles

1. **Lawfulness, fairness and transparency**. You must identify valid grounds under the GDPR (known as a “lawful basis”) for collecting and using personal data. You must use personal data in a way that is fair. This means you must not process the data in a way that is unduly detrimental, unexpected or misleading to the individuals concerned. You must be clear, open and honest with people from the start about how you will use their personal data.
2. **Purpose Limitation**. You must be clear about what your purposes for processing are from the start. You need to record your purposes (we do this by the Student Privacy Notice: <https://dataprotection.leeds.ac.uk/gdpr/student-privacy-notice/>) We must be clear why we are collecting personal data and what we intend to do with it and inform individuals about our purposes.
3. **Data Minimisation.** Data you are processing must be adequate – sufficient to properly fulfil your stated purpose; relevant and limited to what is necessary. You must not hold more than you need for your purposes.
4. **Accuracy.** Personal data we hold must be accurate. We need to keep personal data updated. If you discover that personal data is incorrect or misleading, you must take reasonable steps to correct or erase it as soon as possible.
5. **Storage Limitation.** You must not keep personal data for longer than you need it. We need to be able to justify how long we keep personal data. We do this by the University Retention Schedule available at: <https://dataprotection.leeds.ac.uk/data-protection-and-personal-data/> This considers regulatory and legislative requirements for retaining personal data. You should regularly review the personal data you hold, and ensure it is deleted when you no longer need it.
6. **Integrity and Confidentiality (security).** We must ensure that we have appropriate security measures in place to protect the personal data we hold. We do this by doing a risk analysis of the personal data which will determine where it is located, having appropriate policies – see the Information Protection Policy (IPP) available here: <https://dataprotection.leeds.ac.uk/quick-link-to-resources/> and physical and technical measures such as encryption, and access control. IT regularly test our systems to ensure they have adequate protection. This also relates to physical security – ensuring offices are locked and hard copy documents are locked away securely and ensuring a clean desk policy.
7. **Accountability.** The accountability principle requires you to take responsibility for what you do with personal data and how you comply with the other principles. We meet accountability requirements by ensuring training is available.

## Lawful Basis for Data Processing

GDPR sets out 6 lawful bases for data processing:

Consent

**Contract**

Legal obligation

Vital interests

**Public task**

Legitimate interest

The lawful bases most often used in Student Education Services are contract and public task. Contract can be relied on as a lawful basis if you need to process someone’s personal data to deliver a contractual service to them or because they have asked you to do something before entering into a contract. Students have a contract with the University and often the processing will be to enable the student contract to be fulfilled. Public task can be used as the University is a public authority and the processing is part of its role as a public authority for processing data for teaching and research.

## Which one do I use?

You need to decide but the relevant ones are **consent, contract** and **public task.** You need to document the lawful basis. You can’t change your mind once this has been decided! The Privacy Notice should include the lawful basis of data processing and the purposes of the processing. See <https://dataprotection.leeds.ac.uk/> for privacy notices.

## Individual Rights

GDPR provides the following rights for individuals:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling.

**The Right to be Informed**

Individuals have the right to be informed about the collection and use of their personal data. Information must include: purposes for processing their personal data, retention periods for the personal data and who it will be shared with. It must be provided in concise, transparent, intelligible, easily accessible and clear and plain language.

**The Right to Access**

Individuals have the right to access and receive a copy of their personal data. This is referred to as a subject access request – all SARs should be sent to the Secretariat to be dealt with. We must respond within one month of the request.

**The Right to Rectification**

GDPR includes a right for individuals to have inaccurate personal data rectified.

**The Right to Erasure**

GDPR introduces a right for individuals to have personal data erased. This is also known as the “right to be forgotten.”

**The Right to Restrict Processing**

Individuals have the right to request the restriction of their personal data. When processing is restricted, you are permitted to store the personal data, but not use it.

**The Right to Data Portability**

This allows individuals to move, copy or transfer personal data.

**The Right to Object**

GDPR gives individuals the right to object to processing of their personal data.

## What is the University doing?

* GDPR compliance is managed by the Secretariat. A Data Protection Officer has been appointed. There is a new website with advice and templates: [https://dataprotection.leeds.ac.uk](https://dataprotection.leeds.ac.uk/)
* Data Champion network briefings and meetings.
* Reviewing and updating policies – e.g. record retention
* Developing new online training
* GDPR programme of activity to deal with legacy issues in University systems (SAP, Banner etc)

## What should teams and individuals be doing?

* Ensure staff complete the University Information Security Training
* Understand the University personal data classification and ensure personal data is stored securely.
* Ensure all current and new processes are GDPR compliant by adopting “privacy by design” principles
* Data housekeeping
* Delete data when it is no longer needed
* Deal with legacy files on N drive, clear out old e-mails

## Safeguards

* Privacy by design. Data protection by design is about considering data protection and privacy issues upfront in everything you do. This means any system, service, product or process considers privacy and data protection issues at the design phase, and also throughout the lifecycle. It requires you to:
* Put in place appropriate technical and organisational measures designed to implement the data protection principles effectively and
* Integrate safeguards into your processing so that you meet the GDPR’s requirements and protect individual rights. It would apply to:
* Developing new IT systems, services, products and processes that involve processing personal data;
* Developing organisational policies, processes, business practices and/or strategies;
* Embarking on data sharing initiatives; or
* Using personal data for new purposes.

Systems – consider minimisation, anonymization, pseudonymisation, encryption, training and retention schedules.

## Type of data?

Personal data is divided into standard data such as name and address and special category data such as health related, religious belief or political belief, trade union membership, race, ethnic origin, genetics, biometrics, sex life or sexual orientation. Special category data is personal data that needs more protection because it is sensitive. You need to complete a data protection impact assessment (DPIA) for any type of processing which is likely to be high risk. You must therefore be aware of the risks of processing the special category data.

## How do I handle personal data?

* Double check the recipient of your e-mail.
* Double check you have attached the right document.
* Double check that attached spreadsheets do not contain extra tabs or hidden columns.
* Keep filing cabinets and offices locked.

## Get to Know

## 

* The guidance on personal electronic housekeeping: [www.leeds.ac.uk/electronichousekeeping](http://www.leeds.ac.uk/electronichousekeeping)
* The Information Protection Policy: [www.leeds.ac.uk/informationprotection](http://www.leeds.ac.uk/informationprotection)
* The University’s Data Protection website: [www.leeds.ac.uk/dataprotection](http://www.leeds.ac.uk/dataprotection)

## Complete the IT Training

Information Security Essentials is compulsory for all staff. Information Security Advanced is compulsory for all staff who handle sensitive personal information.

## Data Protection Compliance

Only use University approved methods of remote access.

Report data breaches immediately to the IT Service Desk

Encrypt laptops, mobile phones and memory sticks/pen drives

## Classifying Data

**Unclassified data –** unauthorised disclosure would result in no negative impact to individuals or the organisation

**Confidential data –** unauthorised disclosure would have a negative impact on individuals or the organisation e.g. some identifiable personal data.

**Highly confidential –** unauthorised disclosure would result in serious damage to an individual e.g. release of special category data.

## Unclassified data

* Anonymous data
* Publically available information e.g. staff directory
* List of names with no other personal data
* Final degree classifications

## Classified/Confidential

* Individual’s personal information e.g. passport details, home address
* List of student names plus their student ID and/or e-mail
* Attendance details relating to an existing student
* Exam scripts, exam marks, student transcript

## Classified/Highly Confidential

* Financial information
* Individual’s name plus date of birth, national insurance number, home address and telephone number
* Special category data e.g. ethnicity, disability, health, sexual orientation
* Disciplinary information
* Preliminary degree classification or transcript information pending approval

## Student Privacy Notice

[www.leeds.ac.uk/privacynotice](http://www.leeds.ac.uk/privacynotice)

**We tell students that we will:**

* Process their personal data for the administration of their position as a student in the delivery of the student contract
* Limit access to personal data to those employees, agents, contractors and third parties who have a business requirement to know.
* Put in place appropriate security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed.
* Only retain personal information for as long as is necessary to fulfil the purpose we collected it for.

## Releasing Data

* If contacted by a third party about student data it should not be released unless you have clarified we have permission to release it e.g. we may need the student’s consent first.

## Data Protection Impact Assessments

* What is this?
* A risk assessment in terms of the data
* ICO has screening checklists to decide on whether needed.
* Needed were processing “**likely to result in a high risk to individuals”** ICO website

## How do I assess the risk?

* Consider the likelihood and severity of any impact on individuals
* Consult the Data Protection Officer
* You may need to consult your data processors on the risk
* Very high risk processing should consult the ICO before it starts

## Data Protection Impact Assessment

* Carry out a DPIA if:
* You process large amounts of special category data.
* Use new technologies.
* Process biometric or genetic data.
* Combine, compare or match data from multiple sources.
* Process personal data in a way which involves tracking individuals’ online or offline location or behaviour.
* Process children’s personal data or offer services directly to them.
* Process personal data in a way which could result in a risk of physical harm in the event of a security breach.
* Systematic processing of sensitive data or highly personal data.
* Processing on a large scale.
* Processing data of vulnerable subjects

## Tips

* Consider a DPIA in any major project involving personal data.
* If not using a DPIA document why not.
* Do a new DPIA if there is a change to the nature of processing.

## Example risks

* Loss of personal data
* Uncontrolled access to personal data
* Personal data sent to wrong person
* Misuse of personal data
* Incorrect data associated with a data subject
* Personal data used in a way that might not be expected by the data subject.
* Personal data used without consent
* Personal data kept for longer than required or the published retention period.

|  |  |  |
| --- | --- | --- |
| **Risk** | **Mitigation** | **Result, eliminated, reduced or accepted** |
| Uncontrolled access to classified personal data | Only certain staff are given access to the shared drive where the files are stored. | Eliminated |
| Personal data kept for longer than the University retention schedule | Archive folders will need deleting manually at the appropriate time. The Faculty Programme Support Manager takes responsibility for ensuring this happens | Reduced |
| Loss of personal data | Student data is stored in an N:drive file which is secure. IT monitor information security. The folder is encrypted and therefore not available off campus. | Eliminated. |

## Children

* GDPR has special protections for children
* Design systems and processes with robust protections for them
* Age of consent for consenting to online services in the UK is 13
* Additional parental consent is needed.
* Write clear privacy notices for children so they can understand what happens to their data, and what rights they have.
* Children have the same rights as adults where consent has been used as the legal basis e.g. access, rectification, object to processing and erasure
* The ICO states that the right to erasure is particularly important if data was collected when the individual was a child.

## Sharing data

There are what are called data controllers, and data processors.

* A data controller determines the purposes of the processing of personal data.
* A data processor processes data on behalf of a controller
* If you share data externally a sharing agreement must be in place – there are templates available at: <https://dataprotection.leeds.ac.uk/>
* If you use third party processors a data processing agreement must be in place – templates are available at: <https://dataprotection.leeds.ac.uk/>

## Data Controller

You are a data controller if you:

* Decide to collect or process the data
* Decide the purpose or outcome of the processing
* Decide what personal data should be collected
* Decide which individuals to collect data about
* Have complete autonomy over how the personal data is processed
* Have a direct relationship with the data subjects.

## Data Processor

You are a data processor if you act on behalf of a controller and under their authority. You should only process data in line with a controller’s instructions.

## What is a data breach?

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to personal data.

## Examples

This could include:

* Access by an unauthorised third party;
* Deliberate or accidental action by a controller;
* Sending personal data to the incorrect person;
* Computing devices with personal data on being lost;
* Alteration of personal data without permission.

## Data Breach Reporting

* All data breaches must be reported within 72 hours.
* Report by phone to IT Service Desk (0113 34) 33333.
* If the breach will result in a high risk of adversely affecting individuals they must also be informed.
* All breaches must be reported so they can be logged and we can check for trends.

## Top Tips

* Always bcc students in e-mails.
* Set up lock screen on your PC so that if you leave your desk no-one can access your PC.
* Delete personal information you don’t need.
* Don’t send classified/highly classified content in the body of an e-mail – attach as a file and password protect it.
* Keep filing cabinets locked and the keys secure.

## Questions?

Please contact Alice Temple on [a.c.temple@leeds.ac.uk](mailto:a.c.temple@leeds.ac.uk)