LIVERPOOL JOHN MOORES UNIVERSITY

GDPR

Tel: +44 (0)845 123 3909
www.marshallelearning.com
contactus@marshallacm.co.uk
Metal Box Factory
Great Guildford Street
London, SE1 0HS

MARSHALL
E-LEARNING CONSULTANCY

The General Data Protection Regulation or GDPR, says that personal data, which is information that could identify specific individuals, must be kept safe and secure. This means things like always using passwords, locking away sensitive documents, securely disposing of old information, and enforcing data security. The GDPR has additional requirements covering things like how data is PROCESSED, MADE AVAILABLE, and TRANSFERRED.

To be compliant, you need to make sure you keep data secure and dispose of it safely, review files to make sure they are accurate and still necessary, NEVER disclose data unless authorised, get people's consent wherever possible and provide their data to them on request and make sure data transfers and work by third parties are compliant.

Remember, always be especially careful with sensitive personal data, for example relating to someone's mental health, ethnicity, or sexuality. It is particularly important to seek consent for using this.

Compliance is VITAL because the GDPR has teeth. The Information Commissioner's Office can impose fines of up to €20,000,000, and the damage to the reputation can be enormous. So make sure you know what you're doing. Data underpins everything we do, so it is well worth protecting.

Data protection is a legal responsibility for everyone in our organisation. Complete Sections 1-6 to learn what this means in practice.

1. Data Security
2. GDPR
3. Compliance
4. Rights and Enforcement
5. HE Scenarios
6. Conclusion

Click on the links below for policy documents and further information.

- Guidelines by the Secretariat
- University policies

1. Data Security

Welcome to this resource on the GDPR. This first section introduces the General Data Protection Regulation; it will cover personal data, the ICO's role, and some of the potential consequences of violating the GDPR.

Welcome to the data protection and the GDPR for UK Universities resource. By the end of this, you will be able to:

- Explain what is governed by the GDPR
- Define 'personal data'
- Describe the role of the Information Commissioner's Office (ICO)
- List some of the potential consequences of GDPR violations

The GDPR

The GDPR has been designed to protect data in an era of mass Internet use. It applies across the EU, replacing the different laws (including the Data Protection Act 1998) that previously existed.

The General Data Protection Regulation (GDPR) applies from the 25th May 2018. It (and the new Data Protection Bill) replace the Data Protection Act (1998).

Securing Personal Data

The GDPR governs the use of what is called 'personal data' stating that it must be kept safe and secure. How this applies to Universities:

Personal Data is: 'Any information relating to an identified or identifiable natural person ('data subject') an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.'

Examples of personal data include names, (email) addresses, or someone's date of birth. The GDPR also brings in new things - such as IP addresses. Particular care must be taken with 'special categories of personal data' (e.g., information on someone's physical or mental health, sex life, and now under the GDPR - biometric data).

Information Commissioner's Office (ICO)

The GDPR is enforced and overseen in the UK (and only in the UK) by the

Information Commissioner's Office (ICO) seeks to ensure that organisations keep personal data secure at all times. This means that:

- Passwords should protect all files and digital devices
- Sensitive documents should be locked away whenever they are not in use (and printouts should be picked up promptly)
- Personal data must be sent/transmitted securely
- When it is no longer needed, personal data must be securely disposed of (e.g., shredded or securely deleted)
- When working in public personal data on portable devices/papers is kept confidential and safe

Data Protection isn't just about Data Security. The GDPR has many other requirements that don't relate directly to security (such as how data is processed and made available). We will look at these areas later on, but let's quickly review some case studies showing how vital security issues can be.

1. **Breach:** In 2014, Staffordshire University lost a laptop that held personal data (names, telephone numbers, addresses, and emails) on 125,000 current students (and applicants). The laptop was stolen from a car after a member of staff took it home.

Data Protection Issue: The files were password-protected- but not encrypted. And the laptop should not have been left unattended in a parked car.

2. **Breach:** Essential Travel (a former Thomas Cook subsidiary) lost personal data (including credit card details) belonging to over 1.1 million customers when a hacker broke their website.

Data Protection Issue: In the ICO's words, this was a "staggering lapse" in data security - and it issued a fine of £150,000 after a company admitted it did not have adequate security measures. The organisation hadn't updated anti-hacker defences for six years; hadn't tested its security arrangements; and hadn't deleted out-of-date information.

3. **Breach:** The Bank of Scotland repeatedly sent faxes with sensitive customer details (e.g., names, addresses, bank statements, and other account details) to the wrong recipients over a period of several years, from 2009.

Data Protection Issue: The ICO fined RBS £75,000 for insecure use of its fax machines. The ICO Head of Enforcement said: "To send a person's financial records to the wrong fax number once is careless. To do so continually over three year period, despite being aware of the problem, is unforgivable and in clear breach of the Data Protection Act."

As you will see later, fines under the GDPR have significantly increased. Potential Consequences:

Data breaches (or other violations of the GDPR) can have serious consequences for Universities. The maximum fine level has increased significantly under the GDPR from the previous £500,000 under the DPA.

Reputational damage can also be severe. Based on a recent ICO survey, what do you think the public's reaction would be if a major data breach occurred at a UK organisation?

- Stop using the organisation’s services
- Consider stopping utilizing an organisation’s services
- Would not be concerned at all

The answers are on the following page.

According to the ICO's survey, 20% of the public wouldn't have any more dealings with an organisation, and 57% would consider severing ties. Just 80% of people would have no concerns.

So large fines and serious damage to reputation are definite potential consequences of failing to protect data properly.

2. GDPR Overview

This section provides an overview of the GDPR's core features. It will cover its basic objectives, the key data protection principles, and the main changes in relation to previous legislation. It will also look at the main definitions of some vital GDPR concepts.

By the end of this GDPR overview section, you'll be able to

- List the GDPR's basic objectives
- Describe the GDPR's key data protection principles
- List the main changes in relation to previous legislation
- Define important GDPR concepts

GDPR Objectives:

The GDPR has two main objectives:

- Protection of fundamental rights and freedoms of individual persons with regard to the processing of personal data; and
- Protection of the principle of free movement of personal data within the EU.

As of early 2018, the UK Government has published its new Data Protection Bill, which implement exemptions from the GDPR. The Bill repeals the Data Protection Act 1998 and enshrines GDPR into UK law post-Brexit. It also incorporates a distinct national security regime, gives effect to the Law Enforcement Directive, and creates two new criminal offences.

GDPR Principles

The essence of the GDPR lies in its data protection principles. Each of these principles puts obligations on organisations like Universities to make conscious decisions on how personal information is collected, held, and used.

1. The Lawfulness, Fairness and Transparency Principle

Personal Data shall be processed lawfully, fairly, and in a transparent manner.

There must be a 'lawful condition of processing' which should be fair to the individual and communicated in a clear and transparent way. Typically this means providing a privacy notice to the data subject setting out specific details such as identity and contact details of the Controller, what data is being processed, the purposes and legal basis for processing, and the retention period of the data.

The six lawful conditions for processing personal data are:

- Consent from the data subject
- Necessary for the performance of a contract
- Compliance with a legal obligation
- Protect the vital interests of the data subject (life risk)
- Task carried out in the public interest or official authority
- Legitimate interest of the data controller (this cannot be used for public authority tasks). Additional conditions are required for processing sensitive personal data

2. The Purpose Limitation Principle

Personal Data shall be collected for specified, explicit, and legitimate purposes and not further processed in a manner which is incompatible with those purposes.

Personal data shall be obtained only for one or more specified and lawful purposes.

Personal data can only be used for the specified lawful purpose for which it was collected-just because you have data obtained for one purpose; it doesn't automatically mean you can use it for something else.

However, the GDPR does provide the ability for data to be used for research even when it was not originally collected for that purpose, as long as appropriate safeguards are in place, such as data minimisation and security controls.

3. The Data Minimisation Principle

Personal Data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

Collecting personal data just because it might be needed is not justifiable. Organisations should not hold more information than is needed for the purpose(s) notified.

4. The Accuracy Principle

Personal Data shall be accurate and, where necessary, kept up-to-date.

The best source of information will be from the individual. If this is not possible, an organisation should take reasonable steps to verify it.

Correcting inaccurate information is a fundamental right for individuals- so a process must be in place

to promptly correct information.

5. The Storage Limitation Principle

Personal Data shall be 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 that is no longer needed becomes a risk to any organisation that holds it. How do you know when a personal data is no longer needed? The answer is based on the reason for which it was collected in the first place (it is useful to document this in the Retention Schedule).

When personal data is no longer needed, it must be securely destroyed.

6. The Integrity and Confidentiality Principle

Personal Data shall be 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.

Organisations must make sure that any data held is secure and only accessible to those whose job it is to use it. If personal data is lost or stolen or security breached, an organisation must report it immediately to the appropriate people.

7. The Accountability Principle

The Controller shall be responsible for, and be able to demonstrate compliance with, the Principles.

However, organisations will not only be required to comply with the GDPR- but will also need to proactively demonstrate compliance.

So organisations will need to have things like adequate policies and procedures in place, along with privacy notices and records in place, along with privacy notices and records of processing (usually in the form of an Information Asset Register).

Key GDPR changes

All Universities should be aware of the GDPR's impact, as it contains a number of key changes in relation to previous legislation.

Some of the key area you need to be aware of:

- Consent: Under the GDPR, consent is only required when no other condition of processing applies (such as legitimate interest or compliance with a legal obligation). In this sense, consent is only required as a 'last option' if no other processing reason applies. It is a common misconception that, under the GDPR, explicit consent is required in every situation - but this is not

the case. When it is required, the GDPR has prescriptive rules about what constitutes consent. Where consent is being relied upon, it must be clear, freely given, specific, informed, and active for someone's personal data to be processed. (Broadly speaking for sensitive data, consent must be 'explicit')

Please note that 'opt-out' consent is no longer acceptable: consent should be an active choice to opt-in.

If required, it must be possible to show that someone gave their consent. In addition, data subjects must be able to withdraw their consent.

- Personal Data: The definition of what counts as 'personal data' will expand to include additional factors that might potentially identify a specific individual (e.g., genetic or mental characteristics and social identity, including IP addresses and cookies). Such data may only be collected as far as it is necessary for a specific purpose - and must be erased when that purpose ceases to exist.

- Enhanced Data Subject Rights: These now include the right to:

    - Portability. Personal data must be provided in an electronic format that an individual can easily transfer to alternative data processing systems/another service provider
    - Request that organisations delete their personal data in certain limited circumstances -known as the 'right to be forgotten'
    - Object to their data being used for direct marketing, research, and profiling purposes

  Individuals maintain the right to request copies of any personal data that is held on them. The GDPPR ensures they must receive a response within one month - and for free.

- Accountability: Data Controllers will have to do more to demonstrate that they are compliant in terms of process documentation and privacy notices, impact assessments for 'high risk' data processing, and designing processes to reduce risks (e.g., by minimising the amount of data they need).
- Data Protection Impact Assessment (DPIA): New processing, particularly when there is a high risk to individuals, will require a DPIA to review the risks, impacts to individuals, and protection of the data. The DPO should be consulted, and for very high-risk processing, the ICO may need to be contacted. A DPIA supports building privacy by design and should be carried out at the start of new projects to prevent expensive additional controls being needed later on.

- Expanded Territorial Reach: Unlike the current situation, the GDPR can be enforced where a responsible organisation is established in the EU, even if the actual processing of data is outside the EU. Therefore organisations outside of the EU will be subject to the GDPR if their data processing activities relate to EU citizens, or they monitor the behaviour of data subjects in the EU.

- New obligations on Data Processors: Data Processors will have direct, specific responsibilities (such as actioning new technical requirements). Data Processors can also be liable for

breaches—these are significant changes from the UK DPA. There are also new specific requirements in respect of the contract engaging a Data Processor.

- Mandatory Data Breach Notification Requirements: If a breach occurs, the Data Controller must inform the ICO within 72 hours (unless there is a good reason why this cannot be done). In certain situations, i.e., where there is a high risk to individuals, the data subject(s) must also be informed within 72 hours.

- Appointment of Data Protection Officers: Public authorities (like Universities) must appoint a Data Protection Officer (DPO). The DPO is there to:

    - Advise the University and employees on their data protection obligations.
    - Monitor compliance with the GDPR.
    - Raise awareness and training of staff.
    - Provide advice on issues relating to the protection of personal data (including the Data Protection Impact Assessments).
    - Be the contact point for, and cooperate with the ICO

- Fines and penalties: Under the GDPR, there will be a significant increase in the size of fines and penalties for data breaches.

Definitions Part 1

The GDPR has some key terms which it's useful to understand. Let's start with 'personal data.' Based on your existing knowledge, which of the following definitions seem right?

Select ALL the options you think are correct:

- Personal data = ‘information relating to an identifiable person (living or deceased)’
- Personal data = ‘information relating to a living identifiable person’
- Special categories of personal data = ‘personal data on subjects like an individual’s ethnicity or health’
- Special categories of personal data = ‘personal data on subjects like an individual’s finances’

Definitions Part 2

The GDPR also refers to some key roles and processes. Which of the following definitions seem right to you?

- Controller = ‘the natural or legal person which determines the purposes and means of the processing of personal data’
- Controller = ‘individual which determines what personal data is collected’
- Data Subject = ‘a topic/subject’ of data used by an organization’
- Data Subject = ‘a living person who can be identified by the personal data’
- Processing = ‘refers to any operation performed on personal data, whether or not by automated means’
- Processing = ‘refers to the collection of personal data ONLY’

The answers are on the following page.

Definitions Part 1

The correct definitions. In full, are as follows:

Personal Data refers to information relating to a living identifiable person including expression of opinions about or intentions towards that person.

Special categories of Personal Data refers to personal data that may include information about an individual's racial or ethnic origin; political opinions, trade union status, religious beliefs, health or sexual life or biometric data.

Definitions Part 2

The correct definitions are as follows:

Controller refers to the natural or legal person who determines the purposes and means of

processing of personal data. Data Subject refers to a living, identifiable person

Processing refers to any operation performed on personal data (such as collection, organisation, alteration, retrieval disclosure, erasure, storage and destruction)

• Compliance – Introduction

This section covers how to comply with the requirements of the GDPR. We will start by reviewing how individuals can make sure they are personally compliant, and we will then look at the University's overall GDPR responsibilities.

By the end of this section on GDPR compliance, you will be able to:

- Explain how individuals can ensure GDPR compliance.
- List a University key organisational responsibilities

Compliance: Individuals

Compliance with the GDPR involves establishing a working culture where University staff understand what's a duty of care' for personal data means on a day-to-day basis.

To ensure that you, as an individual, are compliant with Data Protection requirements under the GDPR, you should always try to follow these guidelines.

- **Data disposal**
  Shred paper documents. When electronic records get-out-date- delete them. If you are in charge of getting rid of a work computer(s), ensure that all of the data on it has been deleted.

- **Information security**

  - Always keep personal data secure: lock physical records away, and keep rooms and your screen locked as well (when not in use).
  - Make sure unauthorised people cannot see screens where data is displayed.
  - Follow these steps at home as well as at work.

- **Reviewing files**
  Review files containing personal data regularly. You should only store someone's personal data if it is definitely needed, so if you don't need it anymore, destroy it securely. **Please note: Some data must be kept for legal reasons- so please ensure you are always retaining data in line with the Retention Schedule.**

- **Legal basis for processing**
  You should always make sure you have a legal basis for processing personal data, e.g., the data subject's consent, contractual necessity, or a legal obligation.

- **Individual rights**
  People have the right to see the personal data relating to them held by your organisation - so always aim to be open. **Be aware that individuals can request to see ALL personal data held on them- which includes informal comments (including emails).**

- **Worldwide transfer**
  You must always get someone's permission before you send any of their personal data outside the EU, Norway, Iceland, or Lichtenstein, unless it is to an 'adequate country' or there are other appropriate safeguards in place (e.g., using model transfer clauses approved by the ICO/a supervisory authority).

- **Accuracy**
  Personal data should be accurate, and inaccurate personal data should be rectified without delay (e.g., contact details). **If in doubt, don't use it.**

- **Sensitive data**
  Always be especially careful how you hold and use sensitive personal data (such as mental or physical health, ethnicity, or sexuality). New categories under GDPR include genetic and biometric data. **It is particularly important to seek explicit consent for the processing of this unless other grounds for justification specified by the GDPR apply, e.g., a legal requirement.**

- **Data processors**
  Under the GDPR, a 'Processor' is a natural or legal person, public authority, agency, or other body which processes personal data on behalf of the Controller. Are you using a data processor (e.g., for database management) who needs access to personal data you hold on people? **If so, ensure a written contract exists that states they will handle such data in accordance with the GDPR**

Organisational responsibilities

Under the GDPR, all Universities have several key Data Protection

responsibilities. Universities must:

- Act in compliance with the principles of the GDPR.
- Act in compliance with the data subject rights.
- Ensure there is at least one legal basis for the processing of personal data (or two for Special Categories of Personal Data and criminal convictions).
- Designate individual(s) to be responsible for compliance and, in the case of public authorities, appoint a Data Protection Officer.

Compliance with the GDPR is the responsibility of everyone in an organisation who comes into contact with (and uses) personal data in the course of their work. The most important aspect of compliance is for management to set-and for employees to follow- the organisation's policies and procedures in relation to the processing of personal data.

An organisation must introduce policies, review systems, and train its staff to handle personal data properly, to demonstrate compliance.

Staff should be familiar with their organisation's data protection policy and procedures. However, it is unrealistic to expect that every staff member will understand every part of data protection-so they should know who to consult when questions about personal data arise.

External DPO?

Many organisations will require a Data Protection Officer. Must this be an internal appointment?

Select the option that you think is correct:

- YES – but they can be a part-time employee
- YES – they must be a full-time employee
- NO – they can be an external service provider

The answer is on the next page.

They can be an external service provider (although conflicts of interest must be avoided).
DPOs must be data protection experts. The organisation must support the DPO and provide him/her with the resources necessary to discharge role. The DPO must report to senior management and cannot be penalised or dismissed for performing the role.

• Rights & Enforcement

This section will start by looking at data subject rights, then review how the GDPR is enforced, covering examples of how data breaches may happen and what the potential consequences might be in terms of financial penalties.

By the end of this section on GDPR rights and enforcement, you will be able to:

- List data subject rights
- Explain how the GDPR is enforced
- Give examples of data breaches
- State the potential level of fines for GDPR violations

Beyond data handling

The GDPR isn't just about providing a legal framework to organisations that lays out how they must handle personal data. It also grants rights to individuals to access some of the information that organisations hold on them-and control what is done with it.

The ICO enforces all of this.

Data subject rights

The GDPR is, at its heart, about protecting the privacy rights of the individual. Under the GDPR, 'data subjects' enjoy enhanced rights compared to the Data Protection Act 1998.

- **Access:** Data Subjects have a right to request that a Data Controller supply them with a copy of their personal data. **This includes comments made about them in emails and more obvious personal data held in IT systems.**

  An individual who makes a written request is entitled to be told whether or not any of their personal data is being processed. The rules surrounding what information an individual is entitled to, as well as the timescales for compliance, have changed from the Data Protection Act 1998:

  - In most cases, you will not be able to charge for complying with a request
  - You have one month to comply, rather than 40 days under the Data Protection Act
  - If you refuse a request, you must tell the individual why and that they have the right to Complain to the supervisory authority and seek a judicial remedy. You must do this without undue delay and, at the latest, within one month.

- **Erasure: ('right to be forgotten'):** Individuals have the right to request that organisations delete their personal data in certain limited circumstances.

- **Stop Data Processing:** Restriction of Processing**:** an individual has the right to obtain a restriction of processing in certain limited circumstances.

- **Portability:** This is a new right for data subjects whereby individuals have the right to obtain a copy of their personal data from the Controller in a commonly used format and have it transferred to another Controller.

- **Object to processing:** individuals have the right to object to processing in certain limited circumstances.

- **Automated decision-making:** Individuals have the right to object to significant decisions, including profiling, made solely by automated means.

- **Correct Inaccurate Information:** Rectification. One of the GDPR Principles obliges the Data Controller to maintain only accurate information about individuals. The Data Controller must put in place policies and procedures to ensure that requests to update or change personal data are processed effectively and in a timely fashion.

- **Compensation:** Individuals have a right to claim compensation for damages caused by infringement of the GDPR from the Controller or the Processor.

The ICO

Enforcement of the GDPR is the responsibility of the Information Commissioner's Office (ICO) backed-up by the court system.

The ICO is independent of the government both in administration and funding.

As well as legal enforcement powers, the ICO also issues guidance to encourage good practice to ensure that individuals' rights under the GDPR are upheld.

Data breaches

The GDPR contains a new definition of a 'personal data breach,' which is a breach of security leading to the accidental or unlawful destruction, loss. The alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed.

Examples: loss or theft of equipment, such as a laptop or mobile phone, on which data is stored; or an email containing personal data being sent to the wrong recipient.

Article 32 sets standards for security and processing. Controllers and Processors must implement appropriate technical and organizational measures to prevent breaches, e.g., encryption.

Potential penalties?

One area where the GDPR will introduce significant changes relates to the potential penalties for violations. What do you think the new maximum fine could be?

- €20,000,000
- €15,000,000
- €10,000,000
- €5,000,000
- €4,000,000
- €3,000,000
- €2,000,000
- €1,000,000
- €0

The answer is on the following page.

Under the GDPR there will be an increase in fines to up to 4% of annual turnover (or €20 million) for some failures to comply. This is based on the type and seriousness of breach.

An organization could be fined up to €10,000,000 or 2% of global income if (for example) they fail to: implement measures to ensure privacy by design and default; maintain appropriate security; report breaches; or conduct impact assessments (if required)

They could be fines up to €20,000,000 or 4% of global income if the violation relates to fundamental issues (e.g. breach of the principles of lawfulness, individuals' rights, or conditions for consent).

• HE Scenarios

In this section, you will work through some interactive scenarios based on administrative, research, and teaching activities. These will give you an idea of the types of issues you will need to consider in practice when it comes to the GDPR.

Considerations

It is important to understand that the GDPR shouldn't stop you from doing what you need to in the course of your work at the University.

Instead, it's a case of needing to either get permission to use data in a particular way- or having a legitimate basis for doing so.

Please work through these scenarios based on Administrative, Teaching, and Research activities to get an idea of the kinds of issues you may need to consider.

Admin scenario

Jay works in the University's Administration department. A new Cloud IT system is being set up to run various functions, some of which impact students.

Jay needs to run a number of tests-can these tests use real student data? Select the option you think is correct:

- YES – it would be in the public interest
- NO – this would not be allowed

The answer is on the following page.

Under the GDPR, this would not be OK, as there is no lawful basis for it, it's not in the public interest and permission has not been given by the students. This is also against the principle of 'privacy by design'.

Personal data should not be used in testing unless it has the same full suite of controls as the live system, and is usually only used as a final test process once all other testing has taken place with dummy data.

- YES – it would be in the public interest
- **NO** – this would not be allowed

Admission scenario

Imagine the situation: the Admissions Department want to contact every prospective student who didn't complete an online application to see if they need any help finishing it. Can they do this?

Select the option you think is correct

- NO – this would not be allowed
- YES – there is a lawful basis

The answer is on the following page.

To enable us to support prospective students to enter into a contract with us (and prospective student might reasonably have expected this to happen).However- Admissions shouldn't pester them, so it should be done once.

- NO - this would not be allowed
- **YES** - there is a lawful basis

Teaching scenario #1

A teaching member of staff wants students to volunteer to take part in a research programme- but it is one that doesn't relate to the course of the student they teach. What's the right thing to do here?

Select all options you think are correct:

- Email students who currently attend the University to ask for volunteers.
- Email all students (who have opted-in to receive this type of information) to ask for volunteers.
- Ask the students at the end of the lecture
- Put an ad in a University newsletter

The answer is on the following page.

Students haven't given their permission to be contacted directly for this, and there is no legitimate interest as it doesn't relate to their studies. The member of staff can contact the student body 'as a whole' looking for volunteers- but can't target identifiable people who have not opted-in.

Teaching scenario #2

A member of the teaching staff wants to video a lecture to be available online subsequently. This will involve recording some of the audience too.

What's the right thing to do here?

- Notify the audience in advance
- Announce the recording will occur at the time
- Give the students the right to opt-out

The answer is on the following page.

All of these options, would be a good idea. It's important that opting-out shouldn't disadvantage students – so if this happens, the staff member should give them the opportunity to sit out of range of the videoing, and to ask questions after filming has stopped. However, in some situations this may be hard to do. So-if it's essential-it may be best to build- in permission in the form of a pre-existing contract with the students, so that consent (after that point) isn't required.

Research scenario

An academic researcher has collected data on people for a specific purpose, for which permission was given. Subsequently, another researcher wants to use the same data for other purposes. Is this permissible?

Select the option you think is correct:

- YES – it is permissible
- YES - if the participants are not personally identifiable
- NO – it is not permissible – under any circumstance

The answer is on the following page.

The data could be used for a purpose other than that for which permission was initially given-but only if the participants are not personally identifiable.

- YES - it is permissible
- **YES** - if the participants are not personally identifiable
- NO - it is not permissible – under any circumstance

• Conclusion

You have now reached the end of this resource on Data Protection and the GDPR. If you would like more details on the legal details, please access the full text of the GDPR or additional guidance on the Data Protection Bill.

When you have read through the module workbook, there is an expectation for all staff to complete a short quiz online within LJMU E-Learning modules. Go to https://www.ljmu.ac.uk/staff/ldf/elearning-modules for how to access the modules and further details.