1. What is GDPR?

- The **General Data Protection Regulation** (GDPR) came into force on 25th May 2018, along with the UK's Data Protection Act 2018. Together they introduced a new, comprehensive data protection regime.
- They provide **enhanced rights for individuals** (i.e. you and anyone whose personal data the University holds) regarding their personal information, and **new responsibilities and requirements for organisations** who hold it.

2. What is personal data?

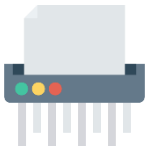
- Personal data is **any information relating to an identifiable individual**.
- An identifiable individual is one who can be identified, directly or indirectly, by reference to an identifier such as a name, identification number, location data, an online identifier or to one or more factors specific to the physical, genetic, mental, economic, cultural or social identity.
- **Special Category Data** is a subset of personal data including especially sensitive information. The rules around using special category data are stricter. It includes racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, physical or mental health, sexual orientation, genetic and biometric data and criminal records.
- **The University holds a very large amount of personal data** – records of students and staff, both present and past, as well as research participants and other individuals, contacts and third parties whose information is needed for the operations of the University. Personal data is found in emails, letters and other correspondence, files and other records, databases and information/records systems, photographs and recordings, contact details, opinions and many other places.
- **All staff will handle personal data so need to be fully aware of requirements and how to handle it appropriately.**

3. The Data Protection Principles

- **At the very heart of GDPR are six data protection principles**. These are golden rules which it's vital to follow them at all times. They say that **personal data shall be**:

1) **Handled in a way that is fair, lawful and transparent –** We need to be upfront and honest with individuals about how we will use their personal data. We can't use it in ways they wouldn't expect and must ensure that we always meet other legal requirements .
2) **Used for specified, explicit and legitimate purposes –** We need to tell individuals what we will do with their personal data, usually by providing data protection/privacy notices (sometimes called fair processing notices). The intended use needs to be reasonable and legitimate, and it would be unlawful to go on and use their personal data for purposes that we haven't specified.

3) **Adequate, relevant and limited to what is necessary** – We can only hold the minimum personal data that we need for the specified purposes, and it would be unlawful to collect and hold any more.
4) **Accurate and up-to-date** – We need to ensure that any personal data we hold is accurate and, where necessary, current.
5) **Kept only for as long as necessary** – We can only hold personal data for as long as we strictly need it for the specified purposes. It must then be securely disposed of or anonymised.



6) **Secure** – It's of vital importance that all personal data the University holds is fully secure.

- The University is required to demonstrate compliance with these principles at all times.

4. Lawful use of personal data

- GDPR sets out six lawful bases, at least one of which must apply to all uses of personal data:

1) **Consent** – If we have an individual's consent to use their personal data for a specific purpose then we are legally able to do so. Consent must be clear, unambiguous, fully-informed and freely given. This will equate to opting in (as opposed to opting out or the use of mechanisms like pre-ticked boxes). However, where as consent may be a direct and obvious way of ensuring that the use of personal data is lawful, much of the University's operations are covered by some of the other options below.

2) **Contract** – If it is necessary to use personal data in a certain way to perform the requirements of a contract then it is permissible to do so. This applies to a student's contract of registration with the University, or a staff member's contract of employment; the University must use their personal data to provide the services and means necessary to fulfil these contractual obligations.

3) **Legal obligation** – The University is legally required to use some personal data it holds in certain ways, for example disclosing some student and staff data to the Office for Students, the Higher Education Statistics Agency (HESA) or similar Government bodies.

4) **Vital interests** – If it's in an individual's vital interests (usually defined as a life or death situation or similar serious scenario where their welfare is at stake), the University can use or share information about them. This lawful basis can apply when information is shared with emergency services.

5) **Public task** – The University's public task is generally defined as teaching and research, as established by the University Charter (itself established by Act of Parliament). Much of the University's activities, if directly related to teaching or research, will be covered by this lawful basis.

6) **Legitimate interests** – Some uses of personal data can be deemed lawful if in the legitimate interests of the individual it relates to.

However, this will only apply in limited circumstances and not if it is also covered by the University's public task.

- A further set of lawful bases are established for the processing of special category data, one of which must apply to make it legal. These include explicit consent of the individual, and use for the purpose of scientific, historical or statistical research, which may cover much of the University's use of this kind of information.

5. Data breaches

- GDPR defines a data breach as, "**a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data**." Examples include:
  - An email or attachment containing personal data being sent to an incorrect recipient
  - A system or service being compromised or hacked due to inadequate security, resulting in personal data being taken
  - Passwords being shared or compromised
  - Documents containing personal data being left unattended and exposed to inappropriate access or misuse, or used in an unauthorised way
  - 'Blagging' - where an individual obtains personal data by deception
  - Failing to ensure that personal data contained in systems can only be accessed by staff with a legitimate operational need to see it
  - Unlawful interception of email or telephone communications
  - Loss or theft of a document, file or electronic device containing personal data
  - Opening a link within a malicious email which contains malware or viruses
  - Cybersecurity or ransomware attack where access to systems or records containing personal data is disabled or encrypted
  - Cc'ing the recipients of an email when they should be Bcc'd due to the need to respect their confidentiality
- If a data breach is likely to result in a risk to the individuals whose data is affected then the University is required to report it to the Information Commissioner's Office (ICO). This needs to happen within 72 hours of discovering the breach.

- If there is a high risk to the individuals whose personal data is involved then the University must also notify them if they are not already aware.
- There are tough penalties if the University is responsible for causing data breaches, including **fines of up to €20million or 4% of turnover**. There could also be serious **reputational consequences** for the University if it suffered a serious or repeated data breach.
- Given the very serious potential penalties, and the requirement to notify the ICO within 72 hours, it is vital that all data breaches and potential data breaches are handled appropriately. **Any staff who believe they have identified a data breach or security incident need to make the Information Governance Team aware without delay by contacting data-protection@bristol.ac.uk or ext.41824**. They will then undertake any necessary investigation, mitigation and reporting.

- Full details of the University's personal data breach procedure can be found on this webpage, including a data breach notification form and advice on actions to take.
- If staff are responsible for deliberate or serious data breaches they could be liable to disciplinary action. Hence, it is vital that you are familiar with requirements.
- **Accessing personal data without permission or using it for purposes unconnected to University business could be a criminal offence**. This could include accessing HR records to view the personal details of a colleague, accessing student records for trivial purposes or to satisfy curiosity, and using someone else's login details for unauthorised purposes.

6. Individuals' data protection rights

GDPR provides all individuals with the following rights regarding their personal data:

- **Right to be informed –** to be told what data what data organisations are collected and holding, and how they are using it, usually provided in the form of data protection/privacy notices (the University's top level notices are published here, but it may be necessary to have local notices as well to cover specific operations).
- **Right of access** – to be provided with a copy of their personal data held by an organisation, subject to some exemptions.
- **Right to erasure** – to have their personal data erased if they withdraw their consent for it to be held and no other legal basis applies, though it is not an absolute right and will not apply in all circumstances. It is sometimes referred to as the right to be forgotten.
- **Right to object –** to their personal data being processed in some circumstances, including for direct marketing.
- **Right to correction –** if inaccurate or incomplete personal data is held.
- **Right to data portability –** to be provided with a digital copy of their personal data to transfer to another organisation, e.g. another university or service provider.
- **Right to object to automated decision-making & profiling –** where profiling or automated means are used to make decisions about them.

If staff receive any requests to exercise any of these rights it's important that they forward them to the Information Governance Team without delay (data-protection@bristol.ac.uk or ext.41824), and do not attempt to respond themselves.

- Requests to access personal data under the right of access are known as 'Subject Access Requests' and can be complicated and time-consuming to handle. They do not need to mention data protection or that it is intended to be a subject access request for it to need to be treated as one. Further information, including a request form can be found on this webpage. **It's vital that the Information Governance Team is made aware of these requests immediately and that you don't try to respond or handle them yourself**.
- Subject access requests will often be made in the context of a dispute (e.g. a staff grievance, student appeal or other complaint, or legal action). The University must respond within one month, although this can be extended for the most challenging requests. There are only limited exemptions that enable information

to be withheld. Remember that anything you write concerning another individual is likely to need to be released to them if they request access.
- Note that subject access requests are different from Freedom of Information requests, which are for recorded non-personal information held by the University and other public authorities.

7. Sharing personal data

- **Only share personal data on a need to know basis and as authorised.** If in doubt check with your manager or the Information Governance Team.
- Don't disclose personal data to a colleague, student or contact unless they are entitled to know. If you unintentionally or deliberately disclose personal data to someone who shouldn't know, or for purposes unrelated to legitimate actions, you could be breaking the law.
- Don't share personal data with external parties without permission, including with official bodies, suppliers, employers, other educational establishments and landlords. **Always check that you are permitted to share the information and that the other party is entitled to receive it.**
- It may not be permissible to share information about students with external parties, including parents and family members, without the student's consent to do so. Some students can be estranged from their families.
- If you receive any approach from the Police or other bodies using statutory powers, don't respond by yourself. Make the Information Governance Team aware of the approach immediately so it can be appropriately managed.
- **Be aware of 'blagging'**, where someone attempts to obtain personal data by deception. Always seek advice if you aren't sure of the identity of another party or the legitimacy of their request.
- **Be aware of 'phishing'**, where fraudsters attempt to obtain valuable information (such as usernames and passwords) by presenting a request as having come from a trusted source. Don't reply to messages asking for personal or financial details, or click on links in emails from unknown sources. Always seek advice if unsure, and report all concerns about phishing to the IT Service Desk.
- **Personal data can only lawfully be transferred outside of the EU when adequate safeguards are in place**. This applies to sending information to students based overseas, accessing your emails from abroad, and using cloud storage which holds data overseas. Please seek advice if you need to transfer personal data overseas outside of established University practices.
- When using personal data always consider whether it can be anonymised or partially anonymised ('pseudonymised') to help protect it. Partial anonymisation can make use of a code or key to obscure identities when it is not strictly necessary to know names or other direct identifiers.

8. Data Protection Impact Assessments

- The University is required to build appropriate measures into its processes, policies and operations to ensure that it fully implements GDPR across all of its activities. This is known as '**data protection by design and default'**.

- To do this, GDPR requires the use of **data protection impact assessments (DPIA)**, a risk assessment exercise designed to identify any risks to the personal data being used, and the individuals it relates to, and establish any actions required to mitigate these risks.
- **A DPIA is legally required when the use of personal data by the University is likely to result in a risk to the individuals it relates to, or when new technologies are being used**. However, it is good practice to undertake a DPIA when a new system or service involving personal data is being introduced, when any changes are being made to existing systems or services, and when planning research involving special category data or large amounts of personal data.
- The University has a **Data Protection Impact Assessment Policy**, which includes a set of screening questions to determine whether a full assessment is required, as well as an assessment form to use to conduct a full DPIA. These documents and further guidance can be found on this webpage.

9. Records retention and disposal

- **GDPR requires that personal data can only be held for as long as is strictly necessary for the purpose intended**. It is illegal to hold it for longer and the University is at risk of regulatory punishment.
- Other types of information should also be securely disposed of when no longer needed, in order to assist with space, cost and efficiency considerations.

- **Information Asset Registers** have been produced detailing all information assets (including personal data) held by divisions, faculties and schools. These registers showed that **over 60% of the University's information assets had no defined retention period or were being held indefinitely**. This is problematic and presents a serious challenge in regard to complying with GDPR.
- In response to this, **a Records Retention Schedule has been produced, detailing how long different categories of record and information should be kept for**. This is accompanied by a Records Management and Retention Policy. It is vital that all areas and levels of the University implement the requirements of these policies, and this will required individual staff members taking responsibility for information held in their area.
- A scanning and offsite storage service has been introduced, enabling paper documents to be securely scanned and held in digital form, or security stored in offsite storage. Please see the Restore service webpages for further details.

10. Information Security

- In order to comply with GDPR, the University and all its staff must practice good information security. The University has a comprehensive Information Security Policy and it is the responsibility of all staff to adhere to it fully at all times. Taking the following steps will assist with this.

- Lock your screen so you don't display any confidential information when you are away from it for any period of time. You never know who could view it when you are not in attendance.
- Don't download or use software, apps or services with personal data or other confidential information that aren't provided by the University, or you don't have formal permission to use. T his includes using cloud storage services, such as Dropbox.
- Don't connect hardware or devices to the University network without formal permission to do so.
- The University has policies covering the use of portable storage devices (e.g. USBs, portable hard disk drives), cloud storage services, and file sharing programmes/services designed to protect its network and information, so please check before you make use of these.
- Take extra care when sending emails. A large portion of the personal data breaches suffered are due to a lack of due care and attention when sending emails. Use Bcc instead of Cc if the confidentiality of recipients needs to be protected.
- If sending personal data or special category data to an external recipient you should apply appropriate protection. Sending it within an encrypted attachment, rather than the body of the email, is usually a suitable easy option.
- Apply sensible password management by making them long but not too complex to remember. Don't write passwords down. Make them difficult to guess and not based on information about you that could be easily found out (e.g. date of birth or address). Using the first letters from words in a meaningful phrase or song lyric, coupled with numbers and symbols, will usually produce a secure password.
- Don't share passwords and don't use your University password(s) for any other accounts, as this parents a risk to University information if they are compromised.
- Don't leave paper documents featuring personal data or other confidential information exposed when you aren't present. Lock them away.
- Dispose of paper documents containing personal data or other confidential information securely, using the University's secure disposal service.
- Don't send confidential content via regular post, but instead use a courier or secure delivery service. If sending portable media devices via the post ensure they are fully encrypted.
- It may be necessary to take confidential paperwork away from the University, and this can be permissible if appropriate safeguards are employed (check with your supervisor or the Information Governance Team). Keep documents with you or locked away and don't leave them unattended.
- Don't work with confidential information (either on a screen or in paper format) when travelling if others can view it.
- Only use personal devices (e.g. laptops, tablets, mobile phones, portable storage devices) if you have permission to do so. Consult your manager or IT Services if unsure. You may need to ensure that you use a VPN (virtual private network), remote desktop software or mobile device management software. Encryption will be essential if using personal data or other confidential information. Firewalls, anti-virus protection and updates all need to be in place.
- Don't save personal data or confidential information on personal devices that you have permission to use for University business; it should only be securely accessed on the University network and not stored on the device itself. Family and

friends should not be given access to devices used to work on University information.

11. Further resources

- The Information Governance Team in the Secretary's Office (the University's legal team) is responsible for ensuring compliance with data protection laws. This includes maintaining relevant policies, including the University's Data Protection Policy. For guidance and support on data protection matters and any of the contents of this document please get in touch: data-protection@bristol.ac.uk or ext.41824.
- Further information on data protection, GDPR, information security and related issues can found using these resources:
    - The University's Data Protection website - http://www.bristol.ac.uk/secretary/data-protection/
    - The University's Information Governance website - http://www.bristol.ac.uk/secretary/information-governance/
    - The University's Information Security website - http://www.bristol.ac.uk/infosec/
    - Information Commissioner's Office (ICO) website - https://ico.org.uk/

12. Questions

1. Data protection law applies to 'personal data'. Which of the following best describes personal data?
    a. Personal information about staff and students that they have asked the University to keep confidential.
    b. Any information about a living individual from which they can be identified directly or indirectly.
    c. The University's HR files and student records.

2. Your manager asks for your opinion of a colleague who is in their probationary period. You send an email with your views. Which one of the following statements is correct?
    a. Your written opinion about your colleague will be their personal data.
    b. Your email will not be your colleague's personal data as it is only your opinion.
    c. Your email may be your colleague's personal data depending on whether you are critical or not.

3. A colleague in the Admissions team suggests adding a question to the University's registration procedure about students' sexual orientation, on the grounds that it might be relevant information. Which one of the following statements is correct?
    a. This information will allow staff to be sensitive in lectures and seminars when discussing sexual orientation so is important to collect.
    b. The University should not collect more personal data than it strictly needs so it is unlikely to be lawful to collect this information.

c. So long as the University does not discriminate against students depending on their responses it is fine to ask for and retain this information.

4. How long can the University store personal data?
    a. Six years.
    b. For as long as is necessary for the purpose for which it was collected.
    c. Forever
    d. Until the individual it relates to consents to its deletion.

5. Your colleague has access to student contact details and has compiled a list of overseas students' email addresses so that their partner, who works in the travel industry, can contact them with special offers and discounted airfares. Which one of the following statements is true?
    a. Disclosing and using the information for this purpose is a breach of data protection legislation as it is incompatible for the purposes for which it was obtained.
    b. Disclosing and using the information for this purpose is fine as long as your colleague honestly believes that the students would be grateful for the discounts.
    c. Disclosing the using the information for this purpose is fine as long as the students don't object to it.

6. A colleague in the Law School takes photos of students involved in a legal advice clinic and asks you to put them on the University website and see if the local newspaper will publish them to promote the clinic's work. What should you do?
    a. Put them on the website only.
    b. Advise your colleague that you can only publish them as long as the student's faces are pixelated.
    c. Check whether the University's privacy/data protection notices cover this usage. Seek advice on whether consent should be obtained before publishing the photos. Make sure no student has objected to the use of their photo.

7. Which one of the following does a current student or staff member <u>not</u> have the right to do under GDPR?
    a. Obtain a copy of their personal data held by the University subject to any applicable exemptions.
    b. Have incorrect personal data held about them corrected.
    c. Require that the University ceases storing all of their personal data.
    d. Object to the use of their personal data for direct marketing purposes.

8. A student emails you asking for all information that the University holds about them. Which of the following statements is correct?
    a. This is a subject access request and the University must response within a strict statutory timeframe providing the information to which they are entitled.
    b. This will only be a subject access request if the student specifically refers to data protection rights within the email.
    c. This cannot be accepted as a subject access request as it is an email, and not a letter.

9. Personal data contained in emails and letters marked as 'private and confidential' are always exempt from disclosure under a subject access request. True or false?
    a. True
    b. False

10. Your manager asks for feedback on a colleague who recently joined your team. You reply by email endorsing their performance but inadvertently disclose some information about their personal life in their response. Which of the following statements is correct?
    a. Disclosing this information is fine as your manager will treat it confidentially.
    b. You have committed a data breach by sharing personal details about a colleague with someone who did not need to know.
    c. It may be acceptable to share this information depending on how your manager views it.

11. Which of the following would be a strong password for a finance-based system?
    a. PASSWORD
    b. Finance1
    c. MoneyCan'tBuyHappiness££95
    d. Qwertyuiop

12. You need to work from home using hand-written notes containing confidential information about students. Which of the following would be an acceptable way for you to store and access the information?
    a. Email scanned copies of the notes to your personal Gmail account so you can access them from your home PC or laptop.
    b. Scan the notes and store them securely in an appropriate restricted access area of the University network, and use remote access in accordance with IT policy.
    c. Make a paper copy of the notes so if you lose one you still have another.

13. You tend to leave files out on your desk overnight and don't always log out of the University network. However, the only people accessing the room are cleaners. Are your actions appropriate from an information security perspective?
    a. Yes
    b. Only if the cleaners have signed a confidentiality agreement
    c. No

Answers

1. b
2. a
3. b
4. b
5. a
6. c
7. c
8. a
9. b
10. b
11. c
12. b
13. c