Use of Personal Data by Students:

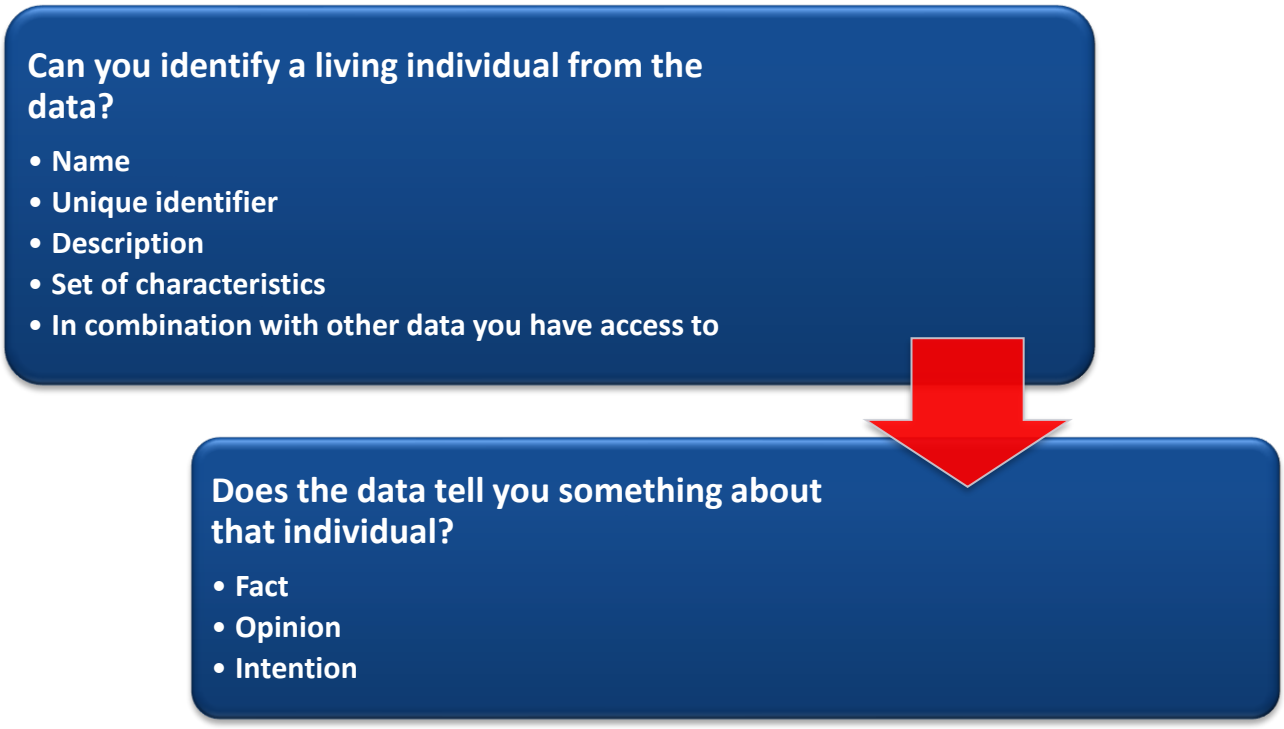
Your Responsibilities

During the course of your studies you may process personal data (i.e. information about an identifiable living individual), for example, you may undertake a survey for a project. Whenever you process personal data you must comply with the requirements of the General Data Protection Regulation (GDPR) and the Data Protection Act 2018. The University is the Data Controller for most of your educational activities and may be fined if personal data is misused and the GDPR is not followed.. The University will view breaches of the Data Protection Act by staff and students seriously and may instigate disciplinary action.

What is personal data?

Personal data is defined by the Information Commissioner's Office (ICO) as, **"any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier."** Identifiers may be name, identification number, location data or online identifier, etc.

If you are unsure as to whether data is personal data, ask yourself 2 questions:



If you answer yes to both questions, the data is personal data.

Data Protection Principles

To comply with the Act you must abide by the data protection principles:

Lawfulness, fairness and transparency	•Comply with the GDPR and any other applicable legislation •Ensure your use of the data is fair to the data subjects •Tell data subjects how you will use their data
Purpose limitation	•Collect data for specific purposes and don't then re-use it for a completely different and incompatible purpose.
Data Minimisation	•Limit the data that you collect to what you really need for your project
Accuracy	•Ensure data is accurate and, where necessary, up to date.
Storage limitation	•Keep personal data only for as long as you need it. Anonymised data can be kept for as long as you like.
Security	•Ensure that personal data is kept securely to avoid accidental loss, destruction, theft and unauthorised access etc.
Accountability	•Underpinning the 6 principles above is the Accountability Principle. The University must be able to demonstrate compliance with GDPR.

These are set out in full in Article 5 of the GDPR - https://gdpr-info.eu/art-5-gdpr/

Privacy Notices

Under GDPR there is a requirement to tell data subjects how their personal data will be used, usually at the point when you collect it from them, e.g. when they complete a questionnaire or a survey for your project/research. There are templates and guidance on the research ethics web pages to help you create a participant information sheet: https://www.shu.ac.uk/research/ethics-integrity-and-practice/research-ethics-approval-procedures. Ask your tutor or supervisor for help.

Security When Handling and Storing Personal Data

The GDPR requires organisations to keep personal data secure (see Data Protection Principles above).

A risk based approach is required, based on the data in question and the circumstances and type of processing.

Appropriate measures may include:

- *robust policies and procedures and ensuring that all staff and students follow these*
- *risk assessments and clear definition of responsibilities*
- *technology - firewalls, anti-virus, anti-hacking technology and measures, password protection of electronic files*
- *locking away paper files, laptops memory sticks etc.*
- *restricting access to offices, databases, filing systems, folders within shared drives*
- *anonymising data where possible and appropriate*
- *using pseudonymisation where possible and appropriate*
- *taking care in open plan offices and at reception desks - face-to-face conversations and telephone conversations*
- *disposing of data securely - shredding, confidential waste, secure disposal of IT equipment etc.*
- *care when working off-campus and using mobile devices*
- *good GDPR awareness and training*

Personal data stored on mobile devices (smartphones, laptops, USB sticks, portable hard drives, dictaphones, tablets etc. **MUST BE ENCRYPTED** to ensure that it remains safe if the portable device is lost or stolen. Contact IT Help if you are not sure whether your device is encrypted: go.shu.ac.uk/itservicedesk

Social media

The data protection rules apply equally to posts on social media. Do not post personal data from projects and research on social media unless you have the consent of the individuals in question.

Data Security Incidents/Breaches

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

personal data. This includes breaches that are the result of both accidental and deliberate causes.

You must report all incidents where there is a risk that a breach has occurred in relation to personal data collected for your **project or research:**

- It is imperative that breaches are reported immediately
- In certain circumstances we may have a duty to report to the ICO
- If the breach happens at SHU you should:
  - contact a member of the faculty
  - call the IT Services Desk on 0114 225 3333 (or visit go.shu.ac.uk/itservicedesk)

If you process personal data for your **placement provider**, eg. patient data, data about children in school, data about your placement provider's clients:

- You should become aware of your placement's reporting policy
- If the breach happens at your placement you should:
  - contact your line manager/placement supervisor
  - follow the policy of your placement setting

If the University, your placement provider, or another **organisation sends you someone else's personal data by mistake:**

- If you are not the intended recipient of data you have an obligation to report this to the sender and delete the data
- If you use the data for another purpose or share the data there may be disciplinary or professional issues and GDPR offence.
- Be mindful of the impact on the data subject(s) - this could be more significant than you realise.

Further Guidance

Undergraduate students carrying out coursework or projects should seek advice from their course tutor or project supervisor and follow applicable research ethics procedures. Post-graduate students writing dissertations should seek advice from their individual supervisor.

Please see the University's Information Governance Policy.

If you are processing personal data for private purposes, you do not need to comply with the University's IG Policy and DP requirements but you still need to abide by other University regulations, for example the University IT Regulations.

For guidance on the encryption of mobile devices see https://shuspace.shu.ac.uk/webapps/portal/execute/tabs/tabAction?tab_tab_group_id=_262_1