Document Title	Code of Practice 1: Collecting and processing personal data – responsibilities of staff
Version	02/12/20
Author	Information Compliance Manager, VCO
Owning Department	Vice-Chancellor's Office
Approval Date	02/12/20
Review Date	31/12/22
Approving Body	Information Assurance and Security Committee
Relevant to	All academic and professional services staff

Introduction: What is personal data?

- Personal data means any information relating to an identified or identifiable living individual (Data Subject), who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data or an online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual.
- A combination of identifiers may be needed to identify an individual.
- Examples include (but are not exhaustive): contact details, Banner ID, an identifiable image of somebody, student marks, email correspondence between people who are discussing a member of staff or student.
- These terms are defined in the General Data Protection Regulation (GDPR) and the Data Protection Act 2018.
- The University is known as the Data Controller.
- The University Secretary, Peter Garrod, is the University's designated Data Protection Officer.
- Sensitive personal data, known as "special category data", is defined as: race, ethnic origin, politics, religion, trade union membership, genetics, biometrics (where used for ID purposes), health, sex life, or sexual orientation.
- The law consists of six principles, as follows in the following numbered paragraphs.
- It is the responsibility of all staff members to comply with the legislation.
- It is also the responsibility of all staff members to supply the Data Protection Officer or their nominee on request with copies of third party personal data held (in response to requests for information from Data Subjects or relevant third parties).

Data Protection Principles

1. **Personal data shall be:**
   (a) processed lawfully, fairly and in a transparent manner in relation to the data subject (the 'lawfulness, fairness, transparency' principle)

This means we must do the following:

- Lawfulness
  - Identify an appropriate lawful basis (or bases) for our processing. There are six options:
    - Consent – bearing in mind that the individual has the right to withdraw consent.
    - Contract with the individual – the individual has the right to object.

        - Legal obligation upon us the University – the individual has the right to erasure of data, portability of data, and to object to that processing.
        - Vital interests (to protect someone's life) – the individual has the right to data portability and to object.
        - Public task (tasks which are the University's official or core functions) – the individual has the right to erasure of data, and to portability of data.
        - Legitimate interests (the University's or a third party's, unless the individual's interests override the institution's) – the individual has the right to data portability.
    - If we are processing special category data or criminal offence data, identify a condition for processing this type of data in addition to one from the list above. The options are as follows (in shortened version):

      (a) explicit consent;
      (b) processing is necessary in the field of employment and social security and social protection law;
      (c) vital interests where the data subject is incapable of giving consent;
      (d) legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim (with provisos);
      (e) personal data made public by the data subject;
      (f) necessary for the establishment, exercise or defence of legal claims;
      (g) reasons of substantial public interest (with provisos);
      (h) necessary for preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, etc.;
      (i) necessary for reasons of public interest in the area of public health, etc.;
      (j) necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes etc.
    - Don't do anything generally unlawful with personal data.
        - This means if processing involves committing a criminal offence, it will obviously be unlawful. However, processing may also be unlawful if it results in:
            - a breach of a duty of confidence;
            - we exceed our legal powers or exercise those powers improperly;
            - an infringement of copyright;
            - a breach of an enforceable contractual agreement;
            - a breach of industry-specific legislation or regulations; or
            - a breach of the Human Rights Act 1998.
        - This list is not exhaustive.
- Fairness
    - Consider how the processing may affect the individuals concerned and justify any adverse impact.
    - Only handle people's data in ways they would reasonably expect, or explain why any unexpected processing is justified.
    - Do not deceive or mislead people when we collect their personal data.
- Transparency
    - Be open and honest, and comply with the transparency obligations of the right to be informed.

- If collecting personal data using a form or questionnaire, or over the phone or in person, a Privacy Notice, sometimes known as a Fair Processing Notice or a Data Protection statement should be used. A template can be found here.

All three of these elements must be satisfied. Conducting a privacy impact assessment should be considered.

2. **Personal data shall be:**
   (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, in accordance with Article 89(1) [GDPR], not be considered to be incompatible with the initial purposes (the 'purpose limitation' principle)

This means we must do the following:

- Clearly identify our purpose(s) for processing – we have a Data Processing Activities Register which sets out our purposes.
- Include details of our purposes in our privacy information for individuals. We have high level Privacy Notices for the information of our students and staff. Privacy notices can be produced for local use as well – refer to the template.
  - Privacy notices should be written in clear language and a style which is aimed at the appropriate audience e.g. student, staff, member of the public, child; and the location where the statement will be placed e.g. online, on social media, on a form, on a notice.
- If we plan to use personal data for a new purpose, we check that this is compatible with our original purpose or we get specific consent for the new purpose.
- In all cases of marketing to individuals, those individuals should be given the opportunity to opt-out.
- When collecting new personal data, or processing personal data in a different way, advice should be sought from Compliance. This could include:
  - Collecting a different set or category of personal data
  - Disclosing personal data to a person or organisation external to the University which is non-routine (especially if outside the European Economic Area)
  - Ceasing to collect personal data or disposing of personal data at a time outside the retention period as stated in the Retention Schedules
  - Processing personal data for a different purpose
  - A privacy impact assessment can be completed to help with these tasks.
- Bear in mind that documents and information for data subjects do not make fundamentally unfair processing fair and lawful.

3. **Personal data shall be:**
   (c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (the 'data minimisation' principle)

This means we must do the following:

- Only collect personal data we actually need for our specified purposes. There should be a valid reason for collecting and using it.
- Have sufficient personal data to properly fulfil those purposes.

- Limit that data to what is necessary – we do not hold more than we need for that purpose. We periodically review the data we hold, by referring to and reviewing our Retention Schedules, and delete anything we don't need.

4. **Personal data shall be:**
   (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 (the 'accuracy' principle)

This means we must do the following:

- Take all reasonable steps to ensure the personal data we hold is not incorrect or misleading as to any matter of fact. If it is we take steps to correct or erase it as soon as possible.
- Have appropriate processes in place to check the accuracy of the data we collect, and know where we obtained the data.
- Ensure the accuracy of any personal data we create.
- Mechanisms should be put in place for checking the accuracy of personal data which is held for any significant length of time
    - E.g. contact details (if they are necessary for keeping in touch with the individual) could be checked on an annual basis. Individuals could be given the opportunity to update their own data.
- Ensure we clearly identify any matters of opinion, and where appropriate whose opinion it is and any relevant changes to the underlying facts. Opinions should be based on facts or evidence.
- Comply with an individual's right to rectification and carefully consider any challenges to the accuracy of the personal data.

5. **Personal data shall be:**
   (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 in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation [GDPR] in order to safeguard the rights and freedoms of the data subject (the 'storage limitation' principle)

This means we must do the following:

- Not keep personal data for longer than we need it.
- Bear in mind that this can include information about individuals included in email correspondence.
- Personal data should be listed on a Retention Schedule, which will include a period for retention.
- If necessary get the data added into the Retention Schedule for the relevant Faculty or Directorate, by referring to the local Records Coordinator.
- Data should be disposed of at the stated time according to the Retention Schedule.
- Bear in mind that individuals have a right to erasure if we no longer need the data.
- We can keep personal data for longer if we are only keeping it for public interest archiving, scientific or historical research, or statistical purposes.

- Bear in mind that personal data kept for longer than necessary are more likely to become out of date, and security risks are increased. There may be unnecessary costs associated with storage and security, also with complying with subject access requests.
- Anonymised data can be kept. Pseudonymising data is useful for complying with data minimisation and security, but individuals may still be able to be identified from it.
- Personal data should not be kept indefinitely 'just in case' it might be useful in future, although it can be kept for archiving, research or statistical purposes.
- Data sharing agreements should be in place when information is shared with other organisations. The agreement should state the retention period of the data for all organisations involved in the data sharing.

6. Personal data shall be:

(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 (the 'confidentiality and integrity' or 'security' principle)

This means we must do the following:

- Undertake an analysis of the risks presented by our processing, and use this to assess the appropriate level of security we need to put in place.
- We have a Privacy Impact Assessment and Information Security Checklist process in place.
- Have the necessary information security and data protection policies in place, and regularly review them.
- Use encryption and/or pseudonymisation where it is appropriate to do so.
- Have an appropriate backup process.
- Ensure that any data processor we use also implements appropriate technical and organisational measures. We may do this through the use of a contract / data sharing agreement.
- Ensure that all staff abide by the security measures, policies and procedures put in place by the University.
- Ensure that staff consider the most appropriate and correct location for the personal data which is under their responsibility, whether that is in hard or soft copy (paper or electronic).
- Ensure that staff consider who should be allowed access to the personal data under their responsibility.
- Ensure that staff protect data against damage or loss, whether accidental or otherwise.
- This could include fire or flood.
- Ensure that staff use the most appropriate method of disposal or destruction of the data at the end of its life.
- Ensure that staff use the most appropriate method of transfer of data, whether in hard or soft copy, and address correctly.
- Ensure that staff do not discuss personal confidential information in public or open plan areas where confidentiality cannot be ensured.
- Ensure that confidential information inadvertently seen or overheard is respected.
- Ensure that hard copy personal data is stored in closed files, not left on desk tops.
- Ensure that sensitive personal data is stored securely at all times.

- Ensure that credit card details or other sensitive financial information is not stored outside the University's central systems.
- Ensure that hard copy sensitive data is stored under lock and key outside working hours.
- Ensure that hard copy personal data when needed to be disposed of is done by shredding or other secure method.
- Ensure that computers are not left logged in if unattended.
- Ensure that care is taken when working on computer screens in public areas or open plan offices, if data can be seen by unauthorised people.
- Ensure that passwords are not shared. Refer to the Password Policy for more information.
- Ensure that when working from home, working on a lap-top or other portable device, and transporting data between sites, the same level of care is taken.
- Staff must complete all mandatory online training modules in Data Protection and Information Security.

Privacy Notice checklist

When writing a Privacy Notice this should include the following:

- Who we are (University of Greenwich) and Data Protection Officer's contact details - Peter Garrod, the University of Greenwich's Data Protection Officer and University Secretary, email: compliance@gre.ac.uk.
- Categories of personal data being processed (e.g. name, contact details, what else?)
- Where did we obtain this data (the Data Subject or someone else, and if someone else, who and how)?
- What is the retention period?
- What are the purposes for processing the data?
- What legal basis / bases are we relying on for processing the data – refer to Principle 1, under "lawfulness" and contact compliance@gre.ac.uk for advice.
- Are we going to share the data with any third party, and are any of those parties overseas?
- A link to their rights as a data subject - https://www.gre.ac.uk/about-us/governance/information-compliance/privacy/data-subject-rights.

Useful links

- Data Subject's Rights
- University of Greenwich Data Processing Activities Register
- Privacy Impact Assessments
- University of Greenwich Privacy Notices and template for a privacy notice
- University of Greenwich Information & Records Retention Schedules
- Marketing Code of Practice
- Data Transfers and Data Sharing Protocol
- Data Classification Policy and other Security policies.