Document Title	Code of Practice 4: Distribution of or access to personal information
Version	18/01/21
Author	Information Compliance Manager, VCO
Owning Department	Vice-Chancellor's Office
Approval Date	18/01/21
Review Date	31/12/22
Approving Body	Information Assurance and Security Committee
Relevant to	All academic and professional services staff

All information which University of Greenwich staff holds and processes should be distributed carefully, according to Data Protection and Freedom of Information rules.

1. **Distributing personal data to University of Greenwich members of staff**

- Staff members are entitled to receive personal data about students or staff if they need the information in order to perform their official duties.
- Distribution should be conducted in the most appropriate and secure manner possible.

2. **Distributing personal data to Hourly Paid Lecturers (HPLs), Job Shop employees, casual workers, temporary agency workers, contractors, interns and those on work experience**

- These categories of employee, worker and other individuals are entitled to receive personal data about students or staff ***only*** if they need the information in order to perform official duties as required by the University.
- Distribution of such data to these categories of employee, worker and other individuals should be conducted in the most appropriate and secure manner possible. This means wherever possible, data is restricted to relevant data only.
- When distributing such data to these individuals, they should be reminded that they must keep the information confidential.

3. **Staff supervising Hourly Paid Lecturers (HPLs), Job Shop employees, casual workers, temporary agency workers, contractors, interns and those on work experience**

- Staff employing or supervising these categories of employees and workers should abide by the following rules: temporary or contract workers without a standard University contract, such as casual workers, volunteers, those on work experience, some internships:
    - These categories of worker should not be granted access to University held personal data (other than data created by themselves or about themselves), unless it is necessary for the fulfilment of their duties. Staff supervising these workers are responsible for ensuring that the University's Data Protection Policy and Codes of Practice are adhered to. To do this they need to ensure that:

        - The individuals understand what personal data is and their responsibility for keeping it confidential.
        - The individuals are aware of the need to protect personal data that they may have access to. This will include:
            - being aware of the best location in which to keep and store the personal data that they may be processing, whether in hard copy or digital copy
            - being aware of how to respond to requests for information, either by telephone, email, in person, or by other means
        - Personal data should be accessed strictly on a need-to-know basis
        - Individuals with access to University systems must complete the Data Protection/GDPR and Information Security on-line training
        - "Browsing" of personal data of any kind, is not permitted. Browsing means accessing data when there is no official reason for doing so. An individual who fails to comply with this, is likely to have their employment, contract or placement with the University terminated
        - Personal data should not be talked about with, or otherwise disclosed to, others, unless it is essential for the fulfilment of their duties as required by the University
        - It should not be taken from University premises or systems
        - It should not be treated carelessly
        - It should not be disposed of without permission
    - Volunteers and work experience staff must not have access to personal data, unless absolutely necessary for the task which they are involved in.
    - Individuals should not have access to sensitive personal data unless absolutely necessary for the task which they are involved in. Sensitive personal data are: race, ethnic origin, politics, religion, trade union membership, genetics, biometrics (where used for ID purposes), health, sex life, or sexual orientation.
- If workers are under the age of 18, supervising staff should familiarise themselves with all duty of care requirements – for further information contact Human Resources.

4. Sharing personal data with collaborative institutions and partners[1]

- When sharing personal data with collaborative institutions and partners, including partner colleges, staff should abide by the following rules. This includes when receiving personal data, as well as providing it:
    - Use only University approved sharing methods and collaboration platforms
    - Ensure proper respect for the confidentiality of data subjects
    - Data subjects should be made aware that sharing is taking place
        - This can be via a Privacy Notice, sometimes known as a Data Protection Statement or Fair Processing Notice
    - Process the data fairly and lawfully
    - There should be a stated purpose for collecting and processing the personal data

[1] For example, franchise arrangements with Further Education Colleges or overseas partners, or research collaborations with other universities.

    - Keep and process it only when necessary and make sure that it is accurate and up to date
    - Take all necessary security measures to protect it, including in transit
    - If transferring the personal data to countries outside the European Economic Area (EEA) make sure that there is adequate protection for the data
- A written data sharing protocol should be set up between organisations or bodies that are sharing personal data. This sets out why data is being shared and sets out the principles and commitments organisations will adopt when they collect, store and disclose personal information about individuals. Template protocol.
- Hourly Paid Lecturers (HPLs), Job Shop employees, casual workers, temporary agency workers, contractors, interns and those on work experience are not permitted to share personal data with collaborative institutions or partners.

5. Transferring personal data abroad

- Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the fundamental rights of the data subject.
    - EEA countries are: Austria, Belgium, Bulgaria, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden.
    - These countries have also been judged as having an adequate level of protection: Andorra, Argentina, Canada, Faroe Islands, Guernsey, Isle of Man, Israel, Japan, Jersey, New Zealand, Switzerland, Uruguay.
    - Regarding the United States, the Information Commissioner's Office will be providing a lawful alternative to the EU-US Privacy Shield, as a contractual basis for data sharing with US processors.
    - The UK is no longer in the EEA or EU. According to the UK-EU Trade and Cooperation Agreement, personal data can continue to flow from the EU (plus Norway, Liechtenstein and Iceland) to the UK for four months from 1st January 2021, extendable to six months.
- When transferring personal data outside the EEA, we must continue to have an appropriate level of protection for the fundamental rights of data subjects:
    - Contract / binding corporate rules etc. (GDPR, Articles 46 & 47)
        - In the absence of these:
    - Explicit consent from the data subject
    - The transfer is necessary for the performance of a contract between data subject and Controller (or in the interest of the data subject)
    - Important reasons of public interest
    - Legal claims
    - To protect the vital interests of someone (where the data subject is incapable of giving consent)
- Hourly Paid Lecturers (HPLs), Job Shop employees, casual workers, temporary agency workers, contractors, interns and those on work experience are not permitted to transfer personal data abroad.

6. Terminating access

When the individual exits the University, their access to systems will be terminated. When the status of an individual changes within the University their authority to access resources must be reviewed and acted upon by their line manager. Refer to the User Account Management and Access Control Policy for further information.

Refer also to:
Code of Practice 1: Collecting and processing data – responsibilities of staff.
The University's Data Classification Policy and information handling procedures.