Document Title	Guidance on conducting a Privacy Impact Assessment (PIA)
Version	06/11/19
Author	Information Compliance Manager, VCO
Owning Department	Vice-Chancellor's Office
Approval Date	19/11/19
Review Date	19/11/21
Approving Body	Information Assurance and Security Committee
Relevant to	All academic and professional services staff

1. Definition of Privacy

Privacy, broadly speaking, is the right to be left alone, or freedom from interference or intrusion. Examples of types of privacy are as follows:
a) data or information privacy – these are rights covered by Data Protection legislation. Individuals have rights in relation to the personal data which is held and processed about them by organisations.
b) privacy of the person in particular, for example having the right to privacy in a toilet cubicle or other private space.
c) privacy of personal behaviour, for example where surveillance (CCTV, for instance) or monitoring is involved.
d) privacy in communications, for example bugging of telephones and monitoring of telephones and emails.

The Human Rights Act guarantees a right to respect for private life which can only be interfered with when it is necessary to meet a legitimate social need.

2. What is a Privacy Impact Assessment?

The University of Greenwich believes that loss of privacy is a risk which must be addressed by building Privacy Impact Assessments (PIA) (sometimes known as Data Protection Impact Assessments (DPIA)) into project management processes and risk management processes. It enables us to fix problems at an early stage, by identifying and minimising privacy risks.

Benefits of conducting a PIA include:

- reassurance for the individual and the organisation,
- procedures are simplified,
- the organisation collects less data,
- costs are lowered,
- awareness of privacy and data protection issues are raised.

3. When staff should conduct a Privacy Impact Assessment (PIA)

Assessments into the risk of a loss of privacy for individuals should be made by staff in certain circumstances, such as the following:

- Projects / plans / proposals
- Administrative systems with privacy implications
- Outsourcing a system to an external supplier

- Methods of electronic communications
- IT systems, which may be designed in-house, or they might be provided by an external supplier
- Sharing of personal data with other bodies external to the University
- Surveys
- New or different use of personal data
- Policies, or statutory duties, which might have a privacy implication
- Whenever there is a potential for damage or distress to individuals

When you don't need to conduct a PIA

PIAs need not be conducted for research projects involving human participants which have gone through research ethics approval. More information here: https://www.gre.ac.uk/research/governance-and-awards/research-ethics-committee. An Information Security Checklist may be required, however, if the research involves software or an external supplier (see point 5 below).

4. Template PIA Document Structure

There are five steps in the conducting of a PIA, as below. The PIA template form is here: https://docs.gre.ac.uk/rep/vco/privacy-impact-assessment-template. The most up-to-date template must always be used. If staff return a PIA using an out-of-date PIA template, they will be asked to use the newest PIA template.

Step One – Identifies the need for a PIA

This is a list of screening questions, which identifies whether there is a need to conduct a PIA (refer to the template, link above).

Step Two – Describes information flows or procedures for the project

This should describe the project, system or process, identifying the purposes for it and how the process will work from beginning to end. It should describe the data subjects involved, the data that will be collected about them, and how that will be managed; how long the data will be kept, and, if third party data processors or partner data controllers are involved, how long they will keep the data.

If Data Subjects need to be given information about the project, system or process, then it may be helpful to put together a Privacy Notice. This can be adapted from the University's template if necessary.

If third party data processors / suppliers or partner data controllers are involved, identify the need for contracts / agreements / data sharing agreements. The University has template agreements which can be used, according to which is the most relevant. The Data Processor Agreement would normally be the default agreement to use, where staff need a template contract for a supplier-type organisation who is acting as a Data Processor on behalf of the University within the UK or EEA (European Economic Area). If the organisation is in the EEA please be aware that there may be Brexit implications at some point. If the third party organisation is, for instance, a research partnership, the Agreement needed is more likely to be a Data Sharing Agreement. The Project Lead should engage with the third party to negotiate a contract, and can get advice from the University Secretary and Data Protection Officer on all these issues, and he will sign the contract when agreed.

Step Three – Identify the privacy risks

Describe what are the risks to individuals and the University. The more intrusion into a person's privacy there is - the higher is the risk of impact, or risk of harm.

Risk arises through personal information being:

- inaccurate, insufficient or out of date,
- excessive or irrelevant,
- kept for too long,
- disclosed to people or organisations that the individual doesn't want their information shared with,
- used in ways that are unacceptable to or unexpected by the person it is about,
- not kept securely,
- transferred outside the EEA which can include being placed on the internet or in the cloud.

Harms for individuals could include:

- financial loss,
- losing a job,
- risks to physical safety,
- damage to personal relationships and social standing,
- identity theft,
- loss of personal autonomy or dignity,
- excessive surveillance,
- legal action,
- distress, including fear of all of the above.

Harms for the organisation include:

- financial damage,
- risk of fines, or other legal action,
- reputational damage,
- loss of business,
- failure of the project or deterioration or changes to the aims of the project.

How to assess the likelihood or impact of a risk

Consider who are the Data Subjects involved in your processing of personal data. The more vulnerable the Data Subject, the higher the likelihood or impact of a risk. A child, or a vulnerable adult, will involve a higher degree of risk. Consider also what is the type of personal data being processed. If it is sensitive ("special category") data, then there is a higher degree of risk. Sensitive personal data is: race, ethnic origin, politics, religion, trade union membership, genetics, biometrics (where used for ID purposes), health, sex life, or sexual orientation. Personal financial information, including credit card details, for instance, will also incur a higher degree of risk. The impact on the individual if they were to sustain a loss or a breach of their data should be considered. For further information on how to quantify a Low, Medium, or High, risk, refer to the Risk Management Guide.

Step Four – Find solutions to the identified risks

Changes to the project / process should be considered at this stage, in order to devise ways to reduce the risks. It is possible that the conclusion will be reached that some risks are necessary. It might be that some risks are not acceptable, and will need to be eliminated. In order to decide whether risks need to be eliminated, or reduced, or accepted, the project outcomes need to be balanced against the impact on individuals. Consider the following:

- Reduction of data collected
- Retention period of data

- Destruction of data
- Security measures
- Staff training and guidance on the system
- Anonymisation or pseudonymisation of data (refer to Code of Practice)
- Data subject awareness / opt out
- Agreements / contracts in place with external data controllers or processors, including data sharing agreements
- Consult with internal / external stakeholders. These people could include: the project team, the University's Data Protection Officer, the designers of the project or system, IT/ILS staff, users of the system.

Step Five – Approval and record-keeping

The completed PIA and associated attachments (which could include copies of contracts, data sharing agreements, and any other illustrative documents such as flowcharts, privacy notices, template correspondence to Data Subjects, etc.) should be sent to compliance@gre.ac.uk. Compliance will endeavour to reply with first comments within 10 working days of receiving a PIA.

The PIA will not be approved until satisfactory answers to all questions put by Compliance have been answered. Therefore plenty of time should be allowed for a PIA to be approved prior to a project / system or process being implemented.

Retrospective PIAs can be conducted, but only for projects, processes or systems which were already in place prior to the PIA procedure being implemented in 2016. New projects, processes or systems should not be commenced without a satisfactory PIA being approved. The Compliance Unit can request a member of staff to conduct a PIA on any project, process or system, if it believes that one should be completed.

If answers are not provided to questions posed regarding the PIA, or if the PIA is not approved, it will be sent to the Information Assurance and Security Committee (IASC) for a decision as to whether the system or project will be disallowed.

If the PIA is approved, it should be integrated into the relevant project plan if necessary. The PIA should be kept as a record by the relevant Project Lead, and a central log of Assessments will be kept by the Vice-Chancellor's Office. Accountability for the recorded risks remains with the project owners.

The Privacy Impact Assessment (PIA) template for staff is here: https://docs.gre.ac.uk/rep/vco/privacy-impact-assessment-template.

5. Information Security Checklist process

It may also be necessary to complete an Information Security Checklist. If the project, process or system involves software, or any IT system or product (whether designed in-house or procured externally to the University), the Checklist should be undertaken. More advice can be obtained from the Information Security team.

The Information Security Checklist template for staff is here: https://docs.gre.ac.uk/rep/information-and-library-services/information-security-check-list.