DATA PROTECTION GUIDANCE HANDBOOK

Contents

1 Glossary

The following terms are used within the Data Protection Policy and Guidance Handbook:

- **Personal Data** – information relating to an identifiable living person ('**data subject**')
- **Processing** – any operation or set of operations carried out on personal data including recording, organisation, storage, adaptation or alteration, retrieval, consultation, disclosure by transmission, dissemination, erasure or destruction.
- **Profiling** – automated processing of personal data to evaluate certain personal aspects relating to a person, in particular to analyse or predict aspects concerning that person's performance at work, economic situation, health, personal preferences, reliability, behaviour or movements.
- **Controller** – organisation, person or other body which alone or jointly with others, determines the purpose and means of processing of personal data.
- **Processor** – organisation, person or other body which processes personal data on behalf of the controller.
- **Third party** – organisation, person or other body, other than the data subject, controller or processor.
- **Consent** – of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by clear affirmative action, signifies agreement to the processing of personal data relating to him or her.
- **Personal data breach** – beach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.
- **GDPR** – EU General Data Protection Regulation

2 Personal Data

Personal data is information about a living individual (the data subject), who is identifiable from that information or who could be identified from that information combined with other data which the University either holds or is likely to obtain. This includes names, contact details, photographs, salary, attendance records, student marks, sickness absence, leave, dates of birth, marital status, personal email address, online identifiers, IP addresses etc. Furthermore any expression of opinion or any intentions regarding a person are also personal data.

The GDPR covers all personal data processed by the University, irrespective of whether these data are held by individual members of staff in their own separate files (including those held outside the University campus e.g. by staff working at home) or in Faculty/Service area records or centrally by the University.

The GDPR separately defines 'special categories of personal data' which relates to the following:

- The racial or ethnic origin of the data subject
- Their political opinions
- Their religious or philosophical beliefs
- Whether they are a member of a trade union
- Their genetic data
- Biometric data used to uniquely identify them
- Their physical or mental health or condition
- Their sex life or sexual orientation

'Special Categories of personal data' can only be processed under limited conditions specified in Article 9 of GDPR. In the context of the University this would most often be:

- The individual has given their explicit consent
- There is a legal requirement to process this information such as immigration or equality requirements
- The processing is required for occupational health, absence management or the provision of health or social care services or treatment
- It is necessary for research or statistical purposes

Whilst not defined in GDPR, there are additional types of personal data which if disclosed could cause significant harm or distress. Examples of these include bank account details, national insurance number, copies of identity documents, date of birth etc.

3 Key considerations

Before embarking on any processing personal data, whether that be sharing personal data with a third party, using a new online tool, marketing a new programme or any other action that involves the use of personal data, you should ask yourself the following questions:

- Do we really need to record the information?
- Could anonymised or pseudonymised data be used?
- Do we have a valid justification for processing the data e.g. it is required for a contract or has the data subject given their consent?
- Has the subject been told about the processing i.e. been issued with a privacy notice?
- Are we authorised to collect/store/process the personal data?
- Have we checked with the data subject that the personal data is accurate?
- Are we sure that the personal data will be secure during the process?
- Are we planning to pass personal data on to a third party or transfer the data outside the EU? If so do we have the necessary contracts/permissions in place to do this?

- If we are setting up new systems/processes have the Data Protection by Design and Data Protection Impact Assessment guidelines been followed?
- Are there alternative ways the same objective can be achieved without using or sharing personal data?

If having considered the points above you conclude that the processing of personal information is necessary then the information in the following sections will provide more details about the factors that need to be considered and the actions that need to be taken to ensure the processing meets the requirements of GDPR.

4 Data Security

The level of security required should be assessed against the risks associated with the data being processed. Security should also be assured no matter where or by whom data is stored or processed and throughout the whole procedure, including the transmission of data. Appropriate measures must be taken to protect against unauthorised or unlawful access.

Staff or students acting on behalf of the University should not place personal data off campus unless absolutely necessary. If it is necessary to place data off campus particular care should be taken to ensure the security of the data. Where information is being held or accessed on a mobile device it should be kept secure at all times with appropriate measures in place to prevent theft or interception of transmission. Where personal data is copied onto a mobile device, additional care is needed to avoid personal data becoming inaccurate over time.

All personal data stored on computer equipment or portable storage media must be deleted beyond retrieval prior to equipment disposal.

Appropriate security measures such as encryption and strong access controls should be used.

See also the separate section 12 on Data Protection by Design.

5 Consent & Privacy Notices

When is Consent needed?

The GDPR requires that all processing of personal information has a lawful basis. Article 6 of GDPR gives a number of circumstances when processing personal information would be justified. See section iv on Conditions of Processing and Consent in the Data Protection Policy for a full list of the lawful reasons for processing. Consent would be used when there is no other lawful basis. This may be the case if we want to use someone's data in a particularly unexpected or potentially intrusive way, or in a way that is incompatible with what we have already told them we will do with their personal data.

The University has two main privacy notices, one for staff and one for students. These notices provide details to staff and students about what they can expect the University to do with their personal information. These privacy notices should cover all types of data processing that are **essential** to manage the relationship the University has with its staff and students and all that happens to personal data while it is held by the University. The majority of what the University does with personal data is necessary to the running of the University and is done in accordance with the official authority vested in the University by its Charter and Statutes and in accordance with the contracts the University has with its staff and students.

Where the University is using personal information in a new way that is not already part of the University's core activities covered by the existing privacy notices, it is likely that we will need to seek consent of the individuals concerned, this includes staff, students or other individuals.

Examples of circumstances when consent would be needed include:

- The use of an **online system or third party organisation** to provide a service to staff or students which includes a requirement to transfer personal details such as staff or student contact details (name, email addresses etc).
- Stories or images of individuals put on the **website** or in publications should have consent.
- Using personal information for **direct marketing** or promotion. GDPR requires that consent is obtained for direct marketing.
- Processing of personal information that includes **special categories** of personal data (sensitive personal data such as religious beliefs, racial or ethnic origin, health conditions, sexual orientation etc) will often require consent.
- One way to legitimise a transfer of personal data **overseas** would be to have consent of the data subjects.

In summary if a new activity is proposed that involves the use of personal data it is likely that consent will be required.

What is Consent?

GDPR defines consent as "any freely given, specific, informed and unambiguous indication of the data subject's wishes which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her." Consent therefore needs to be explicit requiring a positive opt-in (not opt-out, or pre-ticked boxes) and must offer individuals a genuine choice.

Consent that has been obtained must be documented include details of what the individuals were told and when and how they consented.

Individuals must be told that they have the right to withdraw their consent at any time and how to do this.

Privacy Notices

Under the 'fair and transparent' requirements of the first data protection principle, the University is required to provide data subjects with a Privacy Notice to let them know what we are doing with their personal data. If we are carrying out an activity that is not covered by the main staff and student privacy notices of the University then a separate privacy notice will normally need to be provided at the time the personal information is collected or at the same time as consent is sought.

A Privacy notice should include the following information:

- The identity and contact details for the University or any other partner organisations and the contact details for the Data Protection Officer.
- The purpose the data will be used for.
- The legal basis for processing (often consent, where the basis is legitimate interests, contractual or statutory requirements further details must be provided).
- The identity of other people or organisations who may have access to the data.
- Details of any transfers of data outside the EU.
- The retention period of the data or if this is not possible the criteria used to set this.
- The right to access the data, to object to processing or to withdraw consent.

- The right to complain to the Information Commissioner's Office
- Details of automating decision making or profiling where applicable
- Where the personal data has been obtained from if this was not the data subject

A template is included in Appendix 1 to help with the development of a privacy notice but all circumstances are slightly different so the information included in the notice will need to be tailored to the particular circumstance.

If consent is being sought or a privacy notice being prepared in relation to a new activity which could have an impact on the privacy of the individuals concerned then consideration should be given to carrying out a Data Protection Impact Assessment (DPIA). For further information about when and how to do a DPIA please see section 11 on Data Protection Impact Assessments.

6 Research

Personal Data used for research purposes by University staff must be dealt with in accordance with GDPR and its Data Protection Principles. This is subject to the limited exemptions discussed in more detail below. This section outlines the considerations and responsibilities of staff and research postgraduates conducting research involving personal data in the context of the Data Protection Principles. For more information about research conducted by undergraduates and taught postgraduates see section 16 on Personal data processed by students.

The GDPR clarifies that scientific research should be interpreted in a broad manner including privately funded research as well as studies carried out in the public interest. In order for processing to be considered statistical in nature the result of processing should not be 'personal data but aggregate data' and should not be used to support measures or decisions regarding a particular individual.

For information about what is defined as personal data or 'special categories' of personal data see section 3 on Personal Data.

In addition to meeting GDPR requirements, research that involves personal data must still meet the relevant ethical approval procedures.

When using personal data in research it is always best to use anonymised data if possible. However, the level of anonymisation must be such that it is impossible to identify any living individual from the information concerned or in combination with any other information that the University holds or is likely to hold – something which is difficult to achieve. If personal data is suitably anonymised then it is outwith the scope of the GDPR.

Where full anonymisation is not possible then another option is pseudonymisation where the identity of an individual is disguised for instance by replacing identifying fields with artificial identifiers or pseudonyms. When data has been pseudonymised it still retains a level of detail which allows tracking back of the data to its original state. This is in contrast to anomymised data where reverse compilation should be impossible.

The GDPR emphasis that anonymisation or pseudonymisation should be used wherever possible particularly in relation to historical or scientific research or for statistical purposes.

The next few paragraphs lay out the research considerations in relation to the data protection principles.

Principle 1: *Personal data shall be processed lawfully, fairly and in a transparent manner ('lawfulness, fairness and transparency')*

Lawfully
Certain conditions as set out in Article 6 of the regulation must be met before personal data can be processed lawfully. As far as University research is concerned the most likely legal basis for processing personal data will be that it is 'necessary for the performance of a task carried out in the **public interest or in the exercise of official authority** vested in the controller'. Whilst many research participants will be asked to consent to participating in the research from an ethical/confidentiality perspective, it is unlikely that consent will be an appropriate legal basis in relation to GDPR. This is because consent has to be capable of being withdraw. In most research projects once the analysis of data is underway and results are published it would not be feasible to extract the personal data relating to an individual following the withdrawal of consent. In addition research data often gets reused for subsequent research and it is unlikely that consent would be obtainable for this.

Consideration must still be given to participant's rights and interests balanced against the interests in doing the research. If the participants would not reasonably expect the processing, or if it would cause unjustified harm, their interests are likely to override the public interest in doing the research.

When the research involves the use of special categories/sensitive personal data a justification under Article 9 needs to be identified. For research purposes it is likely that Article 9(2)(j) 'public interest, scientific or historical research purposes or statistical purposes' can be used. However for special categories/sensitive personal data further restrictions apply and additions safeguards should be in place (see safeguards paragraph below).

Fair and Transparent
Under the "fair and transparent processing" requirements of the GDPR, researchers also need to provide a Privacy Notice to research participants at the time their personal information is initially collected from them. This Privacy Notice can be combined with a consent form for participating in the research but it should be clear that once they have agreed to participate in the research, consent will not be the legal basis for processing their personal data. For information about what should be included in a Privacy Notice please see section 5 on Consent and Privacy Notices. There are also template 'Participant Information Sheets' which incorporate data protection privacy notice requirements within the 'Ethics template documents' section of the University Ethics webpage.

In some cases, the researcher may be using personal data obtained from a third party, rather than directly from the data subject. In such cases a Privacy Notice should still be provided, unless it can be proved that providing such would be impossible, involve disproportionate effort on the part of the researcher or providing the notice would likely render the research impossible or seriously impair the achievement of the research objectives.

In deciding whether the disproportionate effort argument applies, researchers should evaluate the time, cost and ease of providing the subject with the notice against the benefit to the subject of receiving the notice (or prejudice in not receiving it). Factors to consider in this assessment would include the size of the sample, whether up-to date contact details are available and if not, how easy or practical it would be to obtain them, the purpose of the research and its likely effect on the individuals concerned.

Principle 2: *Personal data shall be collected for specific, explicit and legitimate purposes, and not further processed in any manner incompatible with those purposes ('purpose limitation').*

This principle goes on to state that further processing for archiving, scientific or historical research or statistical purposes is permissible. This is on the basis that the personal data is not used to support measures or decisions regarding any individual and that suitable safeguards have been put in place (see safeguards paragraph below).

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

Researchers should only collect and process personal details which are necessary to conduct their research. For example, if personal identifiers such as names and addresses are not required in order to carry out the research, the respondent should not be asked for such information.

Principle 4: *Personal data shall be accurate and, where necessary, kept up to date ('accuracy').*

Efforts should be made to ensure that personal data gathered for research purposes is accurate. In most research situations it will not be necessary to keep the personal information updated as the research will be based on information representing a situation at a particular moment in time.

Principle 5: *Personal data processed for any purpose or purposes shall not be kept for longer than is necessary ('storage limitation').*

Personal information must be kept in a form which permits identification of data subjects for no longer than is necessary. However, there is an exemption for personal data stored for research purposes provided adequate safeguards are put in place e.g. pseudonymisation, and appropriate technical and organisational measures are in place e.g. the information is stored securely (see safeguards paragraph below)

Principle 6: *Appropriate security including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage using appropriate technical or organisational measures ('integrity and confidentiality').*

Researchers must employ measures appropriate to the sensitivity of the data held to ensure that personal data is kept securely. They should ensure that:

- Personal data held on computer is protected through appropriate access restriction and password protection controls. Digitised personal data should only be stored on shared network drives or University authorised, secure offsite storage (such as Box) and not offline or on local drives.
- Personal data held manually is stored in locked cabinets and offices to prevent accidental or deliberate access by third parties.
- Personal data held off site (e.g. at home or travelling) receives the same level of security protection as it would in the office.
- Personal data is disposed of appropriately once research has been completed. For paper files this will mean disposal in confidential waste sacks for low level personal data, or cross shredding for sensitive personal data. For data held electronically steps should be taken to ensure data is permanently deleted or destroyed.

Safeguards

Research must adhere to both organisational and technical safeguarding measures which mean that:

- You must be able to evidence these safeguarding measures.
- You must be able to prove that your research is in the public interest.
- Your research must not be likely to cause substantial damage or distress to an individual.

Technical and organisational measures are:

- The minimisation principle – use only the absolute minimum of personal data required for your purpose
- Anonymise personal data if you can, if you cannot anonymise, wherever possible, pseudonymise all personal data see Data Protection by Design and Default for more information.
- Store the data securely

Public interest test

- Reasons for any decision that processing is in the public interest should be documented. Relevant considerations could include that the processing is subject to a governance framework which operates with public interest as a criterion, assess independently e.g. peer review from a public funder, REC review or support by the Public Benefit and Privacy Panel for Health and Social Care in Scotland.

Transfers outside the EU

Transfers of personal data to recipients in countries outside the EU are regulated and restricted in certain circumstances. This needs to be taken into account where research involves international collaboration and, in the course of that collaboration, personal data will be transferred to a country outside the EU. In most cases explicit consent for the data transfer will be required from participants. There are some occasions when personal data can be transferred to countries which do not offer an adequate level of protection which include public health research. For more information see section 10 on Transfers of Personal Data outside the EU.

Data Subject Rights

The rights of research participants are restricted. For a full list of rights see section ix on Data Subject Rights in the Data Protection Policy. In some cases there are exemptions from the rights to rectification, to restrict processing, to object to processing, to erasure and the right to access. However these exemptions only apply where it would prevent or seriously impair the achievement of the research, the research is being carried out in the public interest and appropriate safeguards are in place (see paragraph above on safeguards)

Data Protection Impact Assessment

Researchers will need to carry out a Data Protection Impact Assessment if the research could result in a high risk to the rights and freedoms of individuals. This is particularly relevant where research involves a systematic and extensive evaluation of personal aspects relating to individuals and which is based on automated processing, including profiling and which could involve a legal or significant effect on the individual. For further information about when and how to do a DPIA please see section 11 on Data Protection Impact Assessments.

7 Subject Access Requests

Any member of staff receiving a request from an individual for their own personal information should forward this to the Data Protection Advisor as soon as possible (data.protection@stir.ac.uk).

The purpose of the Subject Access rights is to allow individuals to confirm the accuracy of personal data and check the lawfulness of processing to allow them to exercise rights of correction or objection if necessary. The University must respond to all requests for personal information. The following points should help when dealing with a request. In most cases requests should be sent to the Data Protection Advisor for response.

- The request can be in **any format** provided it is clear. The information provided needs to be enough that you are satisfied that you know who they are, that they are that person they say they are, and that the scope of the request is clear

- We should be satisfied about the **identity of the requester** before releasing any information. Proof of identity can be requested if required. A request can be made on behalf of someone else (e.g. a parent or solicitor) *only if* evidence can be provided that the data subject has consented to this. The exception to this would be a young child or vulnerable adult who did not have capacity to make the request themselves.

- If the **scope of the request** is not clear, then we can ask the requester to be more specific about the activities and areas to which the request relates. You can ask them to provide time periods, names of members of staff who may have dealt with them or departments that are most likely to hold the information they are seeking.

- Information must be provided in a **concise, transparent, intelligible** and easily accessible form using clear language.

- The response should be provided in a commonly used **electronic format**, particularly if the request came in electronically, unless the requester asked for another format. When requested by the data subject the information may be provided orally as long as we are confident about the identity of the data subject.

- Information should be provided within **one month**. If the information requested is particularly complex this can be extended by a further two months but the requester must be informed about the extension within one month and the reasons for the delay explained.

- Information must be provided **free of charge** unless additional copies are requested when a reasonable fee can be charged based on administrative costs.

- Where a request is **manifestly unfounded or excessive**, in particular because of their repetitive character the request may be refused. In this case we have to demonstrate how the request is manifestly unfounded or excessive in character.

- The data subject has the **right to obtain the following information**:
    - Confirmation that personal information about them is being processed
    - A copy of that personal information
    - Details of the purpose of the processing
    - Categories of the personal data concerned e.g. does it include any special categories or sensitive personal information?
    - Any recipients or categories of recipients the personal information has been shared with, particularly if these are outside the EU.
    - What safeguards are in place for transfers outwith the EU
    - The period the personal information will be stored for or what the criteria is for determining the period of storage.
    - The existence of the right to request from the controller the correction or deletion of personal data or to restrict or object to the processing of personal data concerning them.
    - The right to lodge a complaint with the Information Commissioner's Office

- What the source of the personal data is if it has not been collected directly from the data subject.
- Details of any automated decision-making, including profiling, and meaningful information about the logic involved and the envisaged consequences of such processing for the data subject.

- The following information should be **redacted** or otherwise removed from a response before it is sent:
  - Personal information relating to other individuals (unless their permission has been obtained to release it or it is otherwise reasonable for it to be released e.g. it is information that the requester already knows).
  - There are also some other exemptions such as information relating to crime and legal proceedings.

For details of how to make a subject access request please see the website https://www.stir.ac.uk/about/faculties-and-services/policy-and-planning/legal-compliance/accessing-information/

8 Data Sharing

Before sharing any personal data with any outside organisation there are a number of things that need to be considered or questions that should be asked.

- Does the data sharing need to take place or could the objective be achieved in other ways?
- Are there any risks involved in sharing the personal data. If there could be, a DPIA should be carried out (see section 11 for details)?
- Does the sharing involve the transfer of data outside the EU (see section 10 for further information)?
- Which condition of processing is being met (see section iv of the Data Protection Policy)?
- Have the data subjects been informed about the transfer via a Privacy Notice (see section 5 on Consent & Privacy Notices)?
- Are all the data protection principles being adhered to (see paragraph 12 of the Data Protection Policy)?
- Is the third party acting as a processor for the University i.e. acting under the instruction of the University? If so there **must** be a contract between the University and the processor.
- Even if the third party is not acting as a data processor there should normally be a contract in place to ensure that the third party is adhering to the data protection principle (e.g. holding the data securely, only keeping the data for as long as is required) and meeting the other legal requirements of GDPR.

Contracts

Data processing contracts or data sharing agreements should contain at least the following information:

- The purpose of the sharing or what processing is being carried out on the data
- The potential recipients or types of recipient and the circumstances in which they will have access
- What data will be shared
- Information about the data quality – accuracy, relevance, usability etc
- Data security
- Retention of the data being shared
- The rights of individuals such as how to make a subject access request or complaint
- Review of effectiveness/termination of the agreement

- Sanctions for failure to comply with the agreement

If you are planning to set up a data sharing or data processing contract you should inform the Data Protection Advisor: data.protection@stir.ac.uk or seek appropriate legal advice.

9 Requests for Personal Information from Third Parties

The University often receives requests for the personal information on its students and staff from third parties. This section is intended to provide advice to staff on how such requests should be handled to ensure compliance with GDPR.

The University tells students and staff how their information will be used, and in what circumstances and to whom it may be disclosed, through the relevant student and staff privacy notices.

There are some third parties that can require disclosure of personal data, examples of these are in the table below:

Third Party	**Authorisation for disclosure**
UK Funding Councils e.g. HEFCE HEFCW, SFC and their agents e.g. QAA, HESA, HEFCE auditors	Further and Higher Education Act, 1992 s.79
Electoral registration officers	Representation of the People Act 2000; The Representation of the People (Scotland) & (England and Wales) Regulations 2001
Officers of the Department of Works and Pensions, and Local Authorities	Social Security Administration Act 1992: s.110A, s.109B and s.109C
Health and Safety Executive	Reporting of Injuries, Diseases and Dangerous Occurrences Regulations (RIDDOR) 1995 s.3
Audit Commission and related auditing bodies	Audit Commission Act 1998 s.6
Environmental Health Officers	Public Health (Control of Disease) Act 1984 and the Public Health (Infectious Diseases) Regulations 1988
Environment Agency	Agency Regulations – the requester must specify which regulation applies
Child Support Agency (CSA)	Child Support (Information, Evidence and Disclosure) Regulations 1992.
Inland Revenue	Taxes Management Act 1970
Police Officers	With a Court Order
Other third parties	With a Court Order

The University should not process personal information of individuals in ways that are not covered by our privacy notices, or where there is a legal requirement, without explicit consent.

As a general rule, you should never disclose personal data to anyone other than an employee of the University with a legitimate work interest in the information, without consent.

HOW TO HANDLE COMMON TYPES OF THIRD PARTY REQUEST

Requests for references or confirming qualifications

The requestor should be advised that we require explicit consent from the individual concerned before we can release information (in relation to students it is important not to confirm whether or not the student has attended the University prior to consent being obtained).

The consent must be in writing (letter or email) and include sufficient information (full name, address, date of birth, dates and subjects of study/areas or work) to allow us to identify them, and be satisfied as to their identity. A letter should be signed or, for a current student or member of staff, an email from their University of Stirling email account will be sufficient evidence of identity.

In instances where the third party seeking information suspects an individual has falsely claimed to have a qualification from Stirling, the Data Protection Advisor (data.protection@stir.ac.uk) should be consulted.

Requests from parents, friends or relatives
No release without explicit consent of the student.

It is acceptable to advise them that we will accept a message and, if having checked our records and such a person exists, will pass it on. This avoids disclosing any information about the student, including whether or not they are at the University.

Requests from organisations providing financial support
The University routinely notifies public funding bodies and the Student Loans Company of changes to a student's status. These disclosures are covered in our privacy notices and records of processing activities. Records should not be disclosed to organisations that are not covered in our privacy notices (e.g private funders) without evidence of student consent.

Requests from Home Office/Immigration and Nationality Directorate/UK Visas
The University often receives requests for information on attendance and other details relating to international students. Information should only be disclosed where we are satisfied there is a legal requirement to provide the requested information or the individual concerned has given their consent.

Requests from the Police or law enforcement officials
The University is not legally obliged to provide information to the police, unless presented with a court order. However, the University may choose to release information where the police, or other law enforcement agencies, can demonstrate to our satisfaction that non-release would be likely to prejudice the prevention/detection of crime or apprehension/prosecution of offenders.

The University will aim to support police investigations where possible. However, the University is obliged to manage personal information in accordance with GDPR.

Requests from the police should:

- be in writing
- be signed and counter signed, the latter by a senior officer
- be for specific information about a specific individual. While this may not always be the case, the information requested should be relevant and limited.
- state that the personal data requested are required for the stated purposes and that failure to provide the information will, in their opinion, be likely to prejudice the investigation.

The Data Protection Advisor (data.protection@stir.ac.uk) should be informed when such requests have been received.

Disclosures required by law
There are circumstances where the University is legally obliged to disclose information about an individual to a third party if this is required by law, enactment or court order (see table above for examples of these cases).

With such requests, we must ensure that any legal obligation (details of legislation and relevant section) is correctly described by the requestor in writing.

All such requests should be referred to the Data Protection Advisor for advice and validation.

Information provided for Council Tax purposes
The University routinely provides the local Councils with details of current students for Council Tax exemption purposes. Students living outwith such council areas may ask for certification for this purpose and we are legally obliged to provide them with this.

Occasionally, students object to this processing and request that we do not pass their details to the Council. They are entitled to do so under the GDPR and the University would have to stop processing the information in this way unless it can be demonstrated that there are compelling legitimate grounds for processing which override the interests, rights and freedoms of the data subject.

Any objections to processing should be referred to the Data Protection Advisor for advice.

Information about deceased staff or students
GDPR only applies to living individuals, thus a deceased staff or student's personal information is potentially disclosable under the Freedom of Information (Scotland) Act 2002 (FoISA). However, in doing so we must be sure that the individual whose information is sought is in fact deceased and that disclosure does not infringe the data protection rights of any third parties (e.g. parents). There may also be an ongoing duty of confidentiality.

No information should be released unless sufficient evidence of death is provided. Such evidence may include:

- Student or staff member already recorded as deceased on records system
- Notification of death in writing by next of kin
- Obituary or confirmed newspaper report of death (but not if there are insufficient details to conclusively identify the student or staff member on our system)
- Death certificate.

Details of relatives of a deceased student or staff member should not be disclosed.

Consideration should be given to the sensitivities of the deceased individual's family where a request for disclosure is sought in the immediate aftermath of a death (e.g. by the media). Advice should be sought from senior management in such cases.

If it appears that the information may fall within the scope of one of the exemptions under the FoISA, please refer to the Freedom of Information Unit (FOIunit@stir.ac.uk)/Data Protection Advisor (data.protection@stir.ac.uk) for advice.

10 Transfer of Personal Data Outside the EU

Personal data can only be transferred outside the EU if one of the following applied:

- The EU has assessed the third country to have an adequate level of protection. The countries that currently fall into this category are;
    - Andorra
    - Argentina
    - Canada
    - Faeroe Islands
    - Guernsey
    - State of Israel
    - Isle of Man
    - Jersey
    - New Zealand
    - Switzerland
    - Uruguay
- Appropriate safeguards are in place such as a legally binding enforcement instrument, binding corporate rules are in place or there is a contract including the European Commission standard data protection clauses.
- A court or tribunal requires the transfer.
- The data subject has consented to the transfer having been informed of the possible risks of such transfers due to the absence of an adequacy decision and appropriate safeguards. Consent cannot be used for core University business that is part of its public task.
- The transfer is necessary for the performance of a contract between the data subject and the University or in the interests of the data subject between the University and another organisation. A contract with the data subject cannot be used as a justification if the activity is part of the University's core business or public task.
- The transfer is necessary for important reasons of public interest.
- The transfer is necessary for the establishment, exercise or defence of legal claims.
- The transfer is necessary to protect the vital interests of an individual i.e. a life or death situation.
- The transfer is made from a register which is open to the public.

Staff authorising transfers of personal data outside the EU are responsible for ensuring that one of the above requirements is met and ensuring that a record is kept of which condition has been met. Where transfers are done on the basis of consent, evidence of the consent and when it was obtained should be kept.

For more advice on transfers of personal data outside the EU please contact the Data Protection Advisor (data.protection@stir.ac.uk).

11 Data Protection Impact Assessments

A Data Protection Impact Assessment (DPIA) is a process whereby potential privacy issues and risks are identified and examined from the perspective of all stakeholders and allows the University to anticipate and address the likely impacts of new initiatives and put in place measures to minimise or reduce the risks. As the use of technology and the collection and storage of personal data grows, the need to ensure that it is properly managed and maintained increases.

It is a requirement of GDPR that a Data Protection Impact Assessment (DPIA) is carried out in certain circumstances. This section will explain when a DPIA has to be done, how it should be carried out, and what should be taken into consideration as part of the process. The impact assessment covers not

only the protection of personal data but broader privacy of individuals and therefore could also be referred to as a Privacy Impact Assessment (PIA).

The procedures in this section are designed to minimise the risk of harm that can be caused by the use or misuse of personal information by addressing data protection and privacy concerns at the design and development stage of a project. Conducting a DPIA should benefit the University by managing risks, avoiding unnecessary costs, avoiding damage to reputation, ensuring legal obligations are met and improving the relationship with stakeholders.

The term project is used in a broad and flexible way and means any plan or proposal. Examples of the types of projects that need a DPIA are:

- A new IT system storing and accessing personal data
- A data sharing initiative where two or more organisations seek to pool or link sets of personal data
- A proposal to identify people in a particular group or demographic and initiate a course of action (e.g. identifying students believed to be at risk)
- A new surveillance system such as CCTV
- A new database which consolidates information held by separate parts of an organisation

When does a DPIA need to be done?
A DPIA should be done as part of the initial phase of a project to ensure that risks are identified and taken into account before the problems become embedded in the design and causes higher costs due to making changes at a later stage. Also if there is a change to the risk of processing for an existing project a review should be carried out. In the context of this guidance a project could include the development or enhancement of any activity, function or processing such as a system, database, programme, application, service or scheme. The time and effort put into carrying out the DPIA should be proportionate to the risks.

A DPIA does not have to be conducted as a completely separate exercise and it can be useful to consider privacy issues in a broader policy context such as information security. The DPIA does not necessarily need to start and finish before a project can progress further but it can run alongside the project development process.

The GDPR **requires** that a DPIA is carried out in the following cases:

- When the processing involves systematic and extensive evaluation of personal information particularly in cases of automatic processing or profiling[1] where decisions are made that could have a significant or legal impact on an individual.
- When processing on a large scale of special categories of data (see template form in Appendix 2 for details of these categories) or data relating to criminal convictions and offences
- The monitoring of a publicly assessable area on a large scale
- Any other cases specified by the Information Commissioner (none currently specified)

The Assessment
It is the responsibility of the person leading the project to carry out a DPIA. As part of the process the Data Protection Officer must be consulted but it is not the Data Protection Officer who carries out the DPIA.

[1] Profiling is the processing of data to evaluate, analyse or predict behaviour or any feature of their behaviour, preferences or identity.

If your project includes the use of any personal data then you should start by completing the screening questions on the DPIA form (Appendix 2). If the answer to all these questions in 'No' then the remainder of the assessment does not need to be completed but the results from the screening questions should be sent to the Data Protection Officer for recording.

If the response to any of the screening questions is 'Yes' you should go on to complete the remainder of the impact assessment form. Guidance notes are included at the end of the form to help the user ensure that the assessment is properly completed.

The assessment template is split into 8 sections:

- *Project details* – providing a broad overview of the project
- *Details of personal data* – providing details of the types of personal data that will be processed and the justification for this
- *Description of information flows* – how the data will be collected, used, stored and deleted
- *Consultation requirements* – detailing consultation with data subjects or other stakeholders
- *Identification of privacy and related risks* – detailing potential risks
- *Identification of privacy solutions* – what will be done to mitigate the risks
- *Sign off and record of outcomes* – an authorised record of the proposed outcomes
- *Integration of outcomes back into the project plan* – detailing of timing and responsibility for each outcome.

Further information about building privacy into a project during the design stage please see section 12 on Data Protection by Design and by Default.

Once the risks are identified and outcomes and actions agreed it is important that that person leading the project ensures that the necessary actions are implemented. As the project develops and is embedded the privacy risks should continue to be assessed to ensure that adequate protections remain in place.

Once the DPIA process has been completed the outcomes will be recorded in a register maintained by the Data Protection Officer. The register will record each risk, explain what action has been taken or will be taken and identify who is responsible for approving and implementing the solution.

12 Data Protection by Design and Default

Data Protection by design (also called Privacy by design) is an approach to handling personal data that promotes privacy and data protection compliance from the start rather than considered as an after-thought.

All staff and agents of the University are **required** to apply the data protection by design principles when developing a new project or reviewing existing projects that involves the use or storage of personal data. The guidelines below explain the types of project when this might be relevant, what data protection by design is and what measures can be put in please to protect personal data.

Under GDPR the University has an obligation to consider data privacy during the initial design stages of a project as well as throughout the lifecycle of the relevant data processing. By imposing a specific 'privacy by design' requirement, the GDPR emphasises the need to implement appropriate technical and organisational measures to ensure that privacy and the protection of data is not an after-thought.

Examples of the types of projects where privacy should be considered include:

- Building new IT systems for storing or accessing personal data

- Developing policies or strategies that have privacy implications
- Embarking on a data sharing initiative
- Using data for new purposes

This section explains the concept of 'data protection by design' and suggests factors that can be taken into consideration to ensure that the privacy of individuals is protected. This should be read in conjunction with section 11 on Data Protection Impact Assessments.

In addition to meeting legal requirements taking a proactive approach to privacy will reduce the likelihood of fines or financial losses due to data protection breaches and help build reputation and stakeholder confidence.

What is Privacy by Design?
Privacy by Design is an approach to protecting privacy by embedding it into the design specifications of technologies, business practices and physical infrastructure. This means building in privacy during the design phase of any project.

Seven foundation principles of Privacy by Design were first developed by Dr Ann Cavoukian in the 1990s. These can be summarised as:

1	Use **proactive** rather than reactive measures. Anticipate, identify and prevent privacy invasive events before they happen.
2	Privacy should be the **default** position. Personal data must be automatically protected in any system of business practice, with no action required by the individual to protect their privacy
3	Privacy must be **embedded** and integrated into the design of systems and business practices
4	All legitimate interests and objectives are accommodated in a **positive-sum** manner. Both privacy and security are important, and no unnecessary trade-offs need to be made to achieve both.
5	Security should be **end-to-end** throughout the entire lifecycle of the data. Data should be securely retained as needed and destroyed when no longer needed.
6	Visibility and **transparency** are maintained. Stakeholders should be assured that business practices and technologies are operating according to objectives and subject to independent verification.
7	Respect **user privacy** by keeping the interests of the individual uppermost with strong privacy defaults, appropriate notice and user friendly options.

Process
A Data Protection Impact Assessment (DPIA) (see section 11) should be carried out as part of the initial phase of a project or when an existing project is being reviewed. If data protection or privacy implications are identified then measures should be built into the project during the early stages to ensure that risks to privacy are minimised or eliminated.

Below are some examples of measures that can be taken during the project development or review to protect the personal data of individuals, not all these examples will be applicable in all circumstances:

- *Data minimisation* – this includes retention minimisation (only keeping personal data for as long as it is required), collection minimisation (only collecting the personal information that is

needed) and use minimisation (only use personal data when it is absolutely required therefore reducing the chance of individuals being identified).

- *Deletion* – Having automated deletion processes for particular personal data to ensure it is flagged for deletion after a particular period.

- *Anonymisation* – The data is held in a form where the individuals are no longer identifiable and it is unlikely that any individuals can be re-identified by combining the data with other data e.g. data matching. The GDPR emphasises that anonymization or pseudonymisation should be used wherever possible particularly in relation to historical or scientific research or for statistical purposes.

- *Pseudonymisation* – The identity of an individual is disguised for instance by replacing identifying fields with artificial identifiers or pseudonyms. When data has been pseudonymised it still retains a level of detail which allows tracking back of the data to its original state. This is in contrast to anonymised data where reverse compilation should be impossible.

- *Differential privacy* – Random 'noise' is injected into the results of dataset queries to provide a mathematical guarantee that the presence of any one individual in a dataset will be masked. This technique may be useful for research data. Software evaluates the privacy risks or a query and determines the level of noise to introduce into the result before releasing it.

- *Synthetic data* – As long as the number of individuals in the dataset is large enough, it is possible to generate a dataset composed entirely of 'fictional' individuals or altered identities that retain the statistical properties of the original dataset.

- *Privacy by Default* – The system is set up so the default settings are the ones that provide maximum protection against privacy risks i.e. technical and organisational measures are put in place to ensure that, by default, only personal data which are necessary for each specific purpose of the processing are processed. This may mean that the default position would not allow full functionality of the product, unless the user explicitly chooses it.

- *User Access controls* – The amount of personal data that authorised users have access to should be limited to the information they need to know to fulfil their roles.

- *Data subject Access* - Individuals should be able to access their own personal data and be informed of its use and disclosures. If individual users can't access the systems directly themselves it should be set up in a way that allows data to be collated with ease in order to comply with subject access requests.

- *User friendly systems* – Privacy related functions should be user friendly. For instance users should be able to easily update their details or extract information that relates to them.

- *Accuracy* – The design should incorporate checks to ensure accuracy and completeness of data and that it is as up-to-date as is necessary to fulfil the specified purposes.

- *Compliance* – The design should include processes to monitor, evaluate, and verify compliance (e.g. with legal requirements, policies and procedures)

- *State of the art* – State of the art technology and organisation measures should be used where possible, however this needs to be balanced against reasonable costs. Old technology should be replaced where possible and software and patches kept up-to-date. In deciding what measures are appropriate, account should be taken of the nature, scope, context and purposes of processing as well as the risks, likelihood and severity for the rights and freedoms of individuals.

- *Security* – Security measures should include processes for secure destruction, appropriate encryption, and strong access control and logging methods.

- *Suppression of data* – The system should be set up to allow the suppression of data of individuals who have objected to receiving direct marketing or those who want to object to decisions being made about them based on automated processing including profiling. Where appropriate the system should also allow data portability in accordance with the GDPR and the right of individuals to request the transmission of their personal data to another data controller in a machine-readable format.

- *Data processors* – Contracts with data processors need to set out how risk/liability will be apportioned between the parties in relation to implementation of 'privacy by design' and 'privacy by default' requirements.

- *Tenders* – Privacy issues should be considered as part of public tenders.

- *Transfers outside EEA* – Particular consideration should be given to protecting personal data when data is likely to be transferred outside the EEA.

These are some example measure that can be taken and not all of them will be appropriate for every project or system, however, it is likely that most projects will benefit from taking some of the steps outlined above. The DPIA should be used to record the privacy measures that are designed into the project.

13 Direct Marketing

Direct marketing is the communication to a particular individual of any advertising or marketing material. It is not confined to the advertising or marketing of commercial products or services and includes messages trying to sell goods or services and those promoting an organisation or its values or beliefs. Information promoting University events or opportunities for students could constitute direct marketing and therefore it is important that the University is aware of these definitions and regulations particularly when sending out mass communications. This covers all forms of communication including by post, telephone, email and other forms of electronic messages.

It is sometimes difficult to tell the difference between a marketing email and a 'service' email. A service email is a communication that is sent to an individual that facilitates or completes a transaction, whether that is for the sale of goods or services. When trying to identify a service email the following questions should be asked:

- Are we under a legal obligation to send the email?
- Is the email part of the performance of a contract?
- Would the individual be at a disadvantage if they did not receive the email?

If the answer to any of these questions is 'yes' then the email is likely to be more of a services email than a marketing email. For instance an email to a student about an offer of a place on a course, paying fees or how to register would all be examples of service emails.

Marketing emails are those that promote the aims and objectives of the University such as sale of goods, services or organisational ideals. Examples would be details of how to join the sports centre which is not essential information for a student to study at the University.

Any personal details collected and held for direct marketing purposes must comply with the data protection principles e.g. it is fair and lawful, the information is only used for the purpose it is collected for, the information is kept up-to-date, it is not kept for longer than necessary and is held securely.

In addition to GDPR the Privacy and Electronic Communications Regulations 2003 (PECR) regulate in detail the use of electronic communications (e.g. email, SMS text, recorded message) as a form of marketing. PECR is due to be replaced shortly by a new ePrivacy Regulation (ePR).

There are some minor exceptions but in order to comply with the GDPR and PECR requirements governing direct marketing it is safest to assume that consent is required. Consent should normally be obtained when contact details are collected and providing an appropriate privacy notice (see section 5 on Consent & Privacy Notices for more information). The consent must be 'opt-in' and any direct marketing messages should only be sent to those people who have opted in. All subsequent marketing communications that are sent should also contain an option to opt-out with details of how the individual can requests not to receive any further messages. If the University receives an opt-out request it must comply as soon as possible, there are no exceptions to this.

When requesting consent it is good practice to request consent separately for different forms of communication i.e. whether individuals agree to be contacted via post, telephone or email. This is because the different forms of communication are covered by different legislation.

Where direct marketing is communicated by telephone, staff must identify themselves and if requested, provide an address or telephone number on which they can be reached. Where cold-calling for fundraising takes place, details should first be checked against the Telephone Preference Service (TPS). Those receiving calls should be made aware of their right to object to the calls.

There is a small exception to the general opt-in consent rule that is the 'soft opt-in' exception. This is where personal data has been collected in the context of an existing relationship with an individual and the University limits marketing to providing information on similar services/goods. In this case, the soft opt-in allows organisations to market to these individuals via electronic means without having opt-in consent. However, this can only be relied on if the individual was informed at the point of data collection that the information would be used for marketing purposes and they are given the opportunity to opt-out at that stage and in each subsequent piece of communication.

14 Personal Data Breaches

A personal data breach is defined in GDPR to mean:

> "a breach of security leading to the accidental or unlawful destruction, loss, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;"

The University makes every effort to avoid personal data breaches, however, it is possible that mistakes will occur on occasions or things will happen that are beyond the University's control. In these cases it is important that the University responds appropriately. The University has a

responsibility to deal with the breach immediately and appropriately in order to minimise the impact and prevent recurrence. GDPR also imposes a requirement that some personal data breaches are reported to the Information Commissioner's Office within 72 hours of the University becoming aware of the breach.

This section of the Handbook sets out the procedures to follow if a personal data breach is identified. All individuals who access, use or manage the University's information are responsible for following these guidelines and for reporting any data protection breaches that come to their attention.

A personal data breach can occur for a number of reasons some examples of these include:

- Loss or theft of data or equipment on which data is stored;
- Inappropriate access controls allowing unauthorised use;
- Equipment failure;
- Unauthorised disclosure (e.g. email sent to incorrect recipient or document posted to the wrong address or personal information posted onto the website without consent)
- Human error;
- Unforeseen circumstances such as a fire or flood;
- Hacking attack;
- 'Blagging' offences where information is obtained by deceiving the organisation who holds it.

The consequences of a personal data breach could be physical, material or moral damage to individuals such as loss of control over their personal data, identity theft or fraud, financial loss, damage to the reputation, or any other economic or social disadvantage to the individual concerned.

Reporting an incident
It is the responsibility of any member of staff, student or other individual who discovers a personal data breach to report it immediately as follow:

Email: databreach@stir.ac.uk
and
During working hours call the Data Protection Advisor on
Tel: 01786 466940 or 466446

On initial contact the reporter should provide details of:

- The exact nature of the breach
- An indication of the seriousness of the breach (the sensitivity of the data breached, the number of individuals whose data may be involved, who may have access to the data)
- If possible what action needs to be taken immediately to mitigate the breach

The Data Protection Advisor/Officer will ask you to provide more detailed follow up information (see Appendix 3 for further details) within 24 hours of the discovery of the breach.

It will be the responsibility of the University's Data Protection Officer, or their nominee in their absence, to determine if the incident needs to be reported to the Information Commissioner's Office and if so to report it within 72 hours of being notified of the breach.

The Data Protection Advisor/Officer will contact other parties as required such as the University Secretary, the police if there has been any illegal activity or the Communication, Marketing and Public Engagement team if there is likely to be press interest. Other University departments will be notified

as appropriate, in particularly if the breach involves IT security, the Information Services team will also be consulted. There may also be legal/contractual requirements to notify.

Data Subjects
After a personal data breach is identified, the University will assess whether the breach will result in a high risk to the rights and freedoms of individuals and if so to let the data subject know about the breach as soon as possible.

The Data Protection Advisor/Officer will communicate with the area of the University responsible for the data that has been breached and discuss the best way of contacting the data subjects concerned and what information the data subjects should be given.

When individuals are notified they should be given specific and clear advice on what they can do to protect themselves and what support and advice is available from the University. They should be provided with details of who they can contact for further information or to ask questions.

Containment and recovery
Steps should be taken as soon as possible to recover any losses and limit the damage. Steps might include:

- Attempt to recover lost equipment
- Use backups to recover lost, damaged or stolen data
- Change relevant passwords as soon as possible.
- If bank details have been lost/stolen, contacting banks directly for advice on preventing fraudulent use.
- Attempt to retrieve personal data, e.g. recall emails, remove from websites etc

Evaluation and response
Once the incident is contained a review should be conducted into the causes of the breach and the effectiveness of the response. The review should consider the type of data, what protections were in place (e.g. encryption), what happened to the data, whether there could be wider consequences of the breach. If ongoing problems are identified then an action plan should be drawn up to put these right. In the case of the most serious breaches a report will be submitted to the Audit Committee.

If the breach warrants a staff disciplinary investigation HR & Organisation Development will be contacted for advice and guidance.

The Data Protection Advisor will keep a record of all data breaches including the actions taken to mitigate the breach and the lessons learnt.

In the event that University is responsible for causing a personal data breach, or not taking appropriate action to prevent a breach, then there could be financial consequences. It is therefore important to make every effort to prevent breaches occurring and if breaches do occur take required actions. More information about the impact of non-compliance can be found in Section 15.

15 GDPR Fines

Examples of the types of situations when fines can be imposed are provided below.

Fines of up to 20,000,000 euros or up to 4% of global turnover, whichever is higher

- Not complying with the basic principles of processing including conditions of processing
- Not complying with data subject rights

Fines of up to 10,000,000 euros or up to 2% of global turnover, whichever is higher

- Not obtaining the correct consent for processing data
- Failure to implement technical and organisational measure to ensure data protection by design
- Not having correct contracts in place for data processors
- Not maintaining adequate written records
- Failing to report a data breach
- Failure to carry out a privacy impact assessment when required

The level of the fines that could be imposed means there could be serious consequences for the University does not meet the requirements of the GDPR. Fines are likely to be lower if it can be demonstrated that appropriate measures were in place to try and prevent non-compliance.

If data subjects have suffered either material or immaterial damage as a result of an infringement of GDPR there is also the possibility that a claim could be made for financial compensation.

16 Personal data processed by Students

Students use personal data for three main reasons

i. To maintain a personal life, for example to communicate with family and friends
ii. To pursue a course of study with the University, for example to research and write an essay, report or thesis
iii. To carry out research as a member of a University established research group

Students may use many different methods to process personal data, such as maintaining an electronic address book, a computer database, or an email account

When is the University responsible for the personal data processed by students?

The University is only responsible for personal data when it is the data controller for that data. A data controller is the person who determines the purposes for which and the manner in which any personal data is or is to be processed. Therefore the University is only responsible for the personal data processed by students when students process data for the University's purposes. The following are some scenarios that involve students processing personal data.

Scenario One

A student processes personal data in the course of his personal life, for example writing an email (using his university provided email account) to his family about a friend's recent birthday.

The University is not the data controller for personal data processed by the student in the course of his personal life as the University does not determine the purpose of the processing. The fact that the student may choose to use the University provided email account to pursue his personal life does not make the University responsible for the processing of personal data for that purpose. The University did not determine the purpose so the University cannot be the data controller. The student is the data controller and may claim the domestic purposes exemption.

Scenario Two
A student processes personal data in order to pursue a course of study with the University, for example as part of her degree course dissertation the student's supervisor suggests carrying out interviews.

The University is not the data controller for personal data processed by a student to pursue a course of study with the University. Students undertake a course of study with a University for their own personal purposes, most obviously to obtain a qualification. The student is not an employee or agent of the University, and neither does she act on behalf of the University. The student decides what work she will do, the way in which she will do it and what she will include in her final write up. She must make these decisions herself in order to prove that she is capable of degree-level work. She works on behalf of herself and not the University. Thus the University cannot be the data controller for the personal data processed by the student in the course of her studies.

The fact that the student was recommended to undertake interviews by her supervisor does not make the University responsible for the processing of the interviewees' personal data. The role of the supervisor is to advise and teach the student, which includes giving advice on data protection issues as part of the student's training in good research practice, but it was the student's own purpose that the interviews took place.

Scenario Three
A student submits a piece of work (e.g. an essay, report or thesis) in which there is personal data, to the University for assessment.

The University is the data controller for the personal data contained within the submitted piece of work from the point at which it is submitted. Once the work has been submitted the University is responsible for the personal data within the document, for example the member of staff who marks the work is processing the personal data contained within it (by reading it) for the purpose of determining what grade the University should award the student, this is the University's purpose.

Scenario Four
A research student processes personal data whilst working on a project led by a University research group.

The University is the data controller for personal data processed by a student working on a research project led by a University research group. The student processes personal data for the purposes laid down by the project, the remit of which has been decided by the University (or the University employed principal investigator), not the student. The purposes for processing are the University's and not the student's, therefore the University is the data controller and the student is an agent of the University. This is the case whether the student is funded by the research project or whether the student is self-funding. Normally only postgraduate research students would fall under this scenario but not all postgraduate research, in many cases the postgraduate themselves determines the scope of the research and where this is the case the processing is like that described in scenario two.

Therefore the University is the data controller for personal data processed by students in only very limited circumstances.

17 Photographs and recorded images of people

Still and moving images of individuals in small groups can be defined as personal data as they feature identifiable individuals and as a result they have to be processed in accordance with the GDPR principles.

All processing of personal information is required to meet a legal justification in GDPR. In relation to photographs and recorded images this will often mean that consent is required. The sections below explain what is normally required and gives examples of particular circumstances which involve the use of images and recordings.

Not following the guidance below or not obtaining appropriate consent can expose the University to the risk of a legal claim or damage of reputation. If you do not have the consent of the subject then consider using a different image where you know appropriate consent has been obtained.

Scope

These procedures apply to still and moving images and recordings created or commissioned by University employees, contractors or volunteers in the course of their work for the University. The University is the Data Controller for all such images and recordings that feature people, regardless of where the recordings take place. The University determines the purpose of recording and is legally responsible and accountable for its use.

These procedures do not apply to images or audio-visual recordings created by members of the University community or visitors for their own private use on their own personally owned equipment. The University is not the Data Controller for such recordings. However, personal use of images or audio-visual recordings to harass or cause distress to others may be subject to disciplinary sanctions in accordance with other University regulations and policies governing the conduct of staff or students and may also be in breach of criminal law.

When is an image personal data?

Examples of images that are personal data:
Where an individual is the focus of an image the image is likely to be personal data. Examples include:

- photographs of individuals particularly those that are stored with personal details, for example, for identity passes
- photographs of staff or students published on notice boards or websites along with some biographical details
- individual images published in a newsletter or marketing material

Examples of images that are not personal data:
Where individuals are incidentally included in an image or are not the focus, the image is unlikely to contain personal data. Examples include:

- where people are incidentally included in an image or are not the focus, for example at a busy open day, the image is unlikely to classed as personal data
- images of people who are no longer alive; the GDPR only applies to living people so these images are not personal data

General

Small Groups
Where photographs or videos are being taken of individuals or small groups of people then consent should be obtained. This is the easiest and safest way of proving you have obtained the image fairly and in accordance with the individual's rights. There are only a small number of exceptions to this when there is an alternative legal basis for processing such as graduation ceremonies where photographs and filming are done on the basis of contract (see below).

Large Groups
It will usually be enough for the photographer to verbally ask permission to take the photograph to ensure compliance with the GDPR. Anyone not wishing to appear on a group photograph will then have the opportunity to opt out. This approach can be used when photographing, for instance, a seminar. However, if images will be posted on a website explicit consent should be sought as the image will be disclosed outside the EU.

Consent
A sample consent form is included in Appendix 4. If you are using your own consent form it must include details of what the images will be used for, any third parties the images will be share with, whether they will be transferred outside the EU (including posting on websites), how the information will be held securely and for how long, details of the individual rights (e.g. the right to withdraw consent, the right to lodge a complaint with the Information Commissioner's Office) and our contact details (including contact details of the University's Data Protection Officer).

Copies of consent forms should be retained for as long as the image is retained for.

Special Categories of Personal Data

GDPR makes it clear (Recital 51) that photographs are not normally considered to be processing of special categories of personal data (e.g. health information, ethnicity) unless they are being processed by technical means that enables the unique identification of an individual. However care should be taken if images reveal sensitive personal information such as those taken in a medical context. Explicit written consent should be obtained in these circumstances.

Graduation

All students and guests who attend a graduation ceremony are informed in advance that photographs and videos will be taken at the ceremony and that official photographers are likely to be in and around the graduation venue taking photographs and video recording. As part of accepting the invitation to attend the graduation ceremony and agreeing to the graduation terms and conditions students are entering into a contract with the University. The contract makes it clear that there is a possibility that they will be photographed and videoed and for these images to go on the University's website. Students who do not wish to be photographed or videoed have the option to graduate in absentia.

Notices should be placed prominently at the graduation venue so people are aware of the recordings. Notification should advise that official photographs and video recordings are likely to be put on the University's website which means the images are transferred outside the EU. A sample notice can be found in Appendix 5

Photographs taken for purely personal use are exempt from the GDPR requirements so photographs and videos taken by family members at a graduation ceremony are not covered by GDPR.

Other uses of images

ID Cards - Photographs of staff and students are included on ID cards. This is for security purposes and consent is not required. The use of images in this way is covered in the University's Staff Privacy Notice and Student Privacy Notice.

CCTV - CCTV cameras are located around campus for the purposes of security and preventing and detecting crime. Notices are placed around campus advising people of the presence of these cameras.

Research – Images used for research should follow the guidelines on Research in Section 6 and where necessary complete a Data Protection Impact Assessment as part of the project approval process.

Appendix 1 – Template for Privacy Notice

REMOVE OR REPLACE ALL GREY TEXT FROM THE FINAL PRIVACY NOTICE

Purpose
[Include details of what we are doing with the personal information and how it will be used. Provide as much information as possible including details of why we would like to use their details in this way and what the positive benefits might be for them. If we are processing special categories of personal data or will be using information for marketing purposes this should be specified and consent will be required].

Legal Basis
[The data subjects should be told the legal basis that is being used to process their data. This must be one of the following:

- Consent – a consent clause needs to be included at the end of the privacy notice
- Contract – details should be provided of the consequences of not providing any information
- Legal obligation – details of the legal requirement should be provided
- Public task/Official authority – this covers work that University carries out as part of its core functions
- Legitimate interests – this should only be used for activities which are not part of the University's core functions and in this case details should be provided of what interests the University or relevant third party has in the data

In addition if special categories/sensitive personal information is being processed an Article 9 justification needs to be specified.]

Third Parties
[If the personal information will be shared with any individuals or organisations outwith the University details should be provided. If the information will not be shared then it may also be helpful to state this].

Overseas transfers
[If the personal information will be transferred outside the EU details should be provided along with information about what safeguards have been put in place. If any personal information will be placed on a website this should be stated. Note that many online services have servers that are located outwith the EU. Clarification should be sought from the service provider on whether or not this is the case and if so details should be included in the privacy notice.]

Security
[Give details on how the personal information will be stored and what security measures will be in place. For instance, who will have access to it, will it be encrypted, will it be anonymised or pseudonymised?]

Retention
[Give details of how long the personal information will be kept for. If exact details are not known then the basis on which decisions about retention will be made e.g. one year after the end of the project].

[**Profiling –** If automated decision making is carried out details should be included]
[**Sources of data –** Where personal data has not been obtained directly from the data subject details should be provided]

Your rights
You have the right to request to see a copy of the information we hold about you and to request corrections or deletions of the information that is no longer required.

[Where the legal basis for processing is consent] If you provide consent for us to use your personal data in the ways outline above you have the right to subsequently withdraw you consent.

In some circumstance you may have the right to object to the processing of your personal data, to request it is erased where it is no longer required for the stated purposes, or that inaccurate information about you is corrected. For more information about your rights see the Data Protection Policy.

To exercise these rights please use the contact details below

Contact details
If you have any questions relating to this form or the way we are planning to use your information please contact:
[Your Name and area]
University of Stirling, Stirling, FK9 4LA
[Your email address/telephone number]

You have the right to lodge a complaint against the University regarding data protection issues with the Information Commissioner's Office (https://ico.org.uk/concerns/).

The University's Data Protection officer, is Joanna Morrow, Deputy Secretary. If you have any questions relating to data protection these can be addressed to: data.protection@stir.ac.uk in the first instance.

[Where the legal basis for processing is consent a consent clause will need to be included which separately asks for consent for all the different aspects to the processing e.g.]

☐ I consent to the University processing my personal data for the purposes detailed above.

[Or for example]

I agree to my personal information being used for direct marketing purposes via:

☐ Email ☐ Post ☐ Text message

[Where consent is not the legal basis for processing you might include a general agreement clause instead e.g.]

I have read and understand how my personal data will be used.

Signed: ……

Date: ……

Data Classification: Public
Version: v4.0
Publication Date: January 2019

Appendix 2 – Data Protection Impact Assessment Form

Project Title:	
Brief description of the project (if a business case already exists this may be attached)**:**	
Name of Responsible person:	**Position:**
Responsible School/Service:	
Timing of the project (start/end dates, duration, as applicable)	
Date form completed:	

PART 1
Screening questions

	Yes	No
Will the project involve the collection of new information about individuals?		
Will the project compel individuals to provide information about themselves?		
Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?		
Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used for?		
Does the project involve you using new technology which might be perceived as being privacy intrusive? For example the using of biometrics or facial recognition.		
Will the project result in you making decisions or taking action against individuals in ways which can have a significant impact on them?		
Is the information about individuals a kind particularly likely to raise privacy concerns or expectations including special categories data? For example, health records, criminal records or other information that people would consider to be particularly private.		
Will the project require you to contact individuals in a way which they may find intrusive?		
Will the project introduce new facilities that might be used by individuals in the institution to gather, process, analyse or share personal information in ways that would previously have required specialist support?		
Will the project involve the processing of personal data by third parties (third parties would include all cloud based services)?		
Will the project expose personal data to elevated levels of security risks?		
Are stakeholders likely to have privacy concerns about the project?		

If the answer to any of the questions above is 'Yes', Part 2 of the DPIA should be completed. Otherwise, just complete this page and submit a copy to the Data Protection Officer.

PART 2 (see notes at the end for guidance on completing each section)

1) Project details

Explain what the project aims to achieve, what the benefits will be to the University, to individuals and to other parties. You may find it helpful to link to other relevant documents relating to the project, for example a project proposal.

2) Details of personal data

Please indicate what personal data will be collected/stored/processed.

Administration data

Name	☐
Date of Birth/Age	☐
Gender	☐
Contact details	☐
Unique identifier e.g. student number	☐

Other data (please specify):

Special Categories of data

Racial or ethnic origin	☐
Political opinion	☐
Religious or philosophical beliefs	☐
Trade Union membership	☐
Physical or mental health condition	☐
Sexual life and sexual orientation	☐
Genetic data	☐
Biometric data used to identify an individual	☐

Other sensitive information

Financial information/bank account details	☐
Criminal convictions and offences	☐

Other (please specify):

Under Article 6 of the GDPR one of the following conditions needs to apply before the processing is lawful. Please indicate which position applies:

- The individual who the personal data is about has given/will give unambiguous consented to the processing ☐
- The processing is necessary for the performance of a contract with the individual ☐
- The processing is necessary for a legal obligation ☐
- The processing is necessary for the vital interests of someone (i.e. life or death situation) ☐

- The processing is carried out in the public interests or exercise of official authority☐
- The processing is in the legitimate interests of the University or another party and does not prejudice the rights and freedoms of the individual (please provide further details):

If special categories of data are being processed different conditions for processing apply. Please speak to the Data Protection Officer for further information.

3) Describe the Information flows

The collection, use and deletion of personal data should be described here and it may also be helpful to refer to a flow diagram or other way of explaining data flows. You should also say how many individuals are likely to be affected by the project.

4) Consultation requirements

Explain what practical steps you will take to ensure that you identify and address privacy risks. Who should be consulted, internally and externally? How will you carry out the consultation? You should link this to the relevant stages of your project management process.

5) Identification of privacy and related risks

Identify the key privacy risks and associated compliance and corporate risks. Consider whether anything needs to be added to institutional risk registers.

Privacy issue	Risk to individuals	Compliance risk	Associated organisation/ corporate risk

6) Identification of privacy solutions

Describe the actions you could take to reduce the risks, and any future steps which would be necessary (e.g. the production of new guidance or future security testing systems)

Risk	Solution(s)	Result: is the risk eliminated, reduced or accepted?	Evaluation: is the final impact on individuals after implementing each solution a justified, compliant and proportionate response to the aims of the project:

7) Sign off and record the outcomes

Risk	Approved solution	Approved by

8) Integrate the outcomes back into the project plan Who is responsible for integrating the outcomes back into the project plan and updating any project management paperwork? Who is responsible for implementing the solutions that have been approved? Who is the contact for any privacy concerns which may arise in the future?		
Action to be taken	Date for completion of actions	Responsibility for action

Please submit a copy of the completed form to the Data Protection Officer, Joanna Morrow at data.protection@stir.ac.uk

Data Classification: Public
Version: v4.0
Publication Date: January 2019

Notes for completing form

1) Project details
Identify why the project is being planned, what the project is intending to achieve and why it is necessary. As well as providing a clear case for the project as a whole, it should highlight those features that may have the potential to impact on privacy. If other organisations are involved in the processing please say who they are and what their involvement is.

2) Details of personal data
Provide details of the personal data involved, including whether it includes special categories of personal data or other sensitive data. Also provide details of the justification for processing the personal data.

3) Describing the information flows
Describe the information flows of the project, how information is collected, stored, used and deleted. How will data be checked for accuracy and kept up to date. Explain what information is used, what it is used for, who it is obtained from and disclosed to, who will have access, and any other necessary information. If the project involves new links with personal data held in other systems please explain. What security measures will be in place? Will any information be sent off site or transferred outside of the EEA? How will individuals be told about the use of their personal data?

Have similar projects been carried out before, either by the University of other organisations?

4) Consultation requirements
Consultation allows people to highlight privacy risks based on their own area of interest or expertise. It also provides an opportunity for them to suggest measures to reduce the risks. Relevant internal stakeholders should be consulted whilst ensuring their attention is focused on privacy issues. In some cases external consultation may be appropriate. Consultation should be timely, clear, proportionate, reach representative individuals, ask objective questions and seek feedback.

5) Identification of privacy and related risks
Examples of risks include inaccurate, insufficient or out of date information; excessive or irrelevant data; information kept for too long; disclosing the information to someone who should not see it; using information in a way that is unacceptable or unexpected to the person it is about; and information not kept securely. These could cause upset or unnecessary intrusion on privacy. Risks can include risks to physical safety, financial loss or distress caused. Sharing or merging datasets allows the collection of much wider information than an individual might expect.

Some risks will be to the organisation – for example damage to reputation, or the financial costs or a data breach.

Legal compliance risks include the EU General Data Protection Regulation (GDPR), Privacy and Electronic Communications Regulations 2003 (PECR), and the Human Rights Act 1998 (see table below for more details)

6) Identification of privacy solutions
Explain how you could address each risk. Some might be eliminated altogether. Other risks might be reduced. In some cases the chances of risks being realised are small or the impact will be minimal and it may be appropriate to recognise and accept the risks. In these cases the risks should be recorded along with the reasons for accepting the risks.

Evaluate the likely costs and benefits of each approach. Think about the available resources, and the need to deliver a project which is still effective. Consider whether the impact on privacy is proportionate to the aims of the project by balancing the project's outcomes with the impact on individuals. Examples of steps that could be taken to reduce privacy risks include:

- Not collecting or storing some information
- Devising retention periods and planning secure destruction of information
- Using appropriate technology
- Anonymising information when possible
- Producing guidance on the use of the system
- Allowing user access to information so they can correct and access their own data
- Having the necessary agreements in place when data processors are used.
- Having data sharing agreements making it clear what information will be shared and who it will be shared with

For more information about building privacy into a project during the design stages please see the separate guidance on 'Data Protection by Design and by Default'

7) Sign off and record of outcomes
Make sure that the privacy risks have been signed-off at an appropriate level. This can be done as part of the wider project approval.

A DPIA report should summarise the process, and the steps taken to reduce the risks to privacy. It should also record the decisions taken to eliminate, mitigate, or accept the identified risks. Publishing a DPIA report will improve transparency and accountability, and lets individuals learn more about how your project affects them.
8) Integrating of outcomes back into the project plan The DPIA findings and actions should be integrated with the project plan. It might be necessary to return to the DPIA at various stages of the project's development and implementation. Large projects are more likely to benefit from a more formal review process. A DPIA might generate actions which will continue after the assessment has finished, so you should ensure that these are monitored. Record what you can learn from the DPIA for future projects.

Relevant Legislation

EU General Data Protection Regulation (GDPR)	Regulates the processing of personal data – i.e. information about living identifiable individuals
Article 8 of the Human Rights Act	States that everyone has the right to respect for their private and family life, their home and correspondence. This right is qualified, and exceptions relate to national security, public safety or economic wellbeing of the country, prevention of disorder or crime, protection of health or morals, or of the rights and freedoms of others.
Privacy and Electronic Communications Regulations (PECR)	Regulates electronic direct marketing e.g. email and text messages
Regulatory and Investigatory Powers Act (RIPA)	Regulates the interception of communications data (e.g. phone calls, emails and postal letter), their acquisition and disclosure, the carrying out of covert surveillance etc.
Common law duty of confidence	Points to consider are whether: • the information has the necessary quality of confidence; • the information will be given in circumstances under an obligation of confidence; and • there could be an unauthorised use of the information to the detriment of the confider (although detriment does not always need to exist for a breach of confidence to be actionable) There are four sets of circumstances that make disclosure of confidential information lawful • where the individual to who the information relates has given consent; • where disclosure is in the overriding public interest; • where there is a legal duty to do so, for example a court order; • where there is a statutory basis that permits disclosure.

Appendix 3 – Information required in the event of a Data Protection Breach

Details for the data protection breach

Please describe the incident in as much detail as possible.

a) When did the incident happen?
b) How did the incident happen?
c) If there has been a delay in reporting the incident please explain the reasons for this.
d) What measures were in place to prevent an incident of this nature occurring?
e) Please provide extracts from any policies or procedures considered relevant to this incident, and explain which of these were in existence at the time of this incident. Please provide the dates on which they were implemented.

Personal data placed at risk

f) What personal data has been placed at risk? Please specify if any financial or sensitive personal data has been affected and provide details of the extent.
g) How many individuals have been affected and how many data records are involved?
h) Are the affected individuals aware that the incident has occurred?
i) What are the potential consequences and adverse effects on those individuals?
j) Have any affected individuals complained to the University about the incident?

Containment and recovery

k) Has any action been taken to minimise/mitigate the effect on the affected individuals? If so, please provide details.
l) Has the data placed at risk now been recovered? If so, please provide details of how and when this occurred.
m) What steps have been taken to prevent a recurrence of this incident?

Miscellaneous

n) Have the police or any other regulatory bodies been informed about this incident?
o) Has there been any media coverage of the incident?

Appendix 4 – Template Consent form for Photography/Filming

Consent form for photography/filming

I consent to the University of Stirling using photographs and/or video recordings including images of me both internally and externally to promote the University. These images could be used in print and digital media formats including print publications, websites, e-marketing, posters banners, advertising, film, social media, teaching and research purposes.

I understand that images on websites can be viewed throughout the world and not just in the United Kingdom and that some overseas countries may not provide the same level of protection to the rights of individuals as EU/UK legislation provides.

I understand that some images or recordings may be kept permanently once they are published and be kept as an archive of University life.

I have read and understand the conditions and consent to my images being used as described.

Print Name	
Signature	
Date	

The University of Stirling is committed to processing information in accordance with the General Data Protection Regulation (GDPR). The personal data collected on this form will be held securely and will only be used for administrative purposes.

Your rights
You have the right to request to see a copy of the information we hold about you and to request corrections or deletions of the information that is no longer required. You can ask the University to stop using your images at any time, in which case it will not be used in future publications but may continue to appear in publications already in circulation.

You have the right to lodge a complaint against the University regarding data protection issues with the Information Commissioner's Office (https://ico.org.uk/concerns/).

Contact details
If you have any questions relating to this consent form or the way we are planning to use your information please contact:
Communications, Marketing & Recruitment
University of Stirling
Stirling
FK9 4LA
communications@stir.ac.uk

If you have any questions relating to data protection please contact the University's Data Protection Officer, Joanna Morrow, tel: 01786 466940, email data.protection@stir.ac.uk

Appendix 5 – Template for notice of Photography/Filming

Photography/ Filming in Progress

Please note that filming/photography is taking place [at this event/in this area] for promotional and archival purposes. The photographs and recordings made are likely to appear on our website.

If you would prefer not to be photographed please let the photographer know.

For further information contact:
[Name and contact details of event organiser/ representative at the event]

If you have any questions relating to data protection please contact the University's Data Protection Officer, Joanna Morrow, tel: 01786 466940, email data.protection@stir.ac.uk