DATA PROTECTION AUDIT GUIDANCE

CONTENTS

Section I: Audit of Processing of Personal Data
Section II: Audit Procedure

Appendices:

A Audit Form
B List of Purposes
C List of data subjects
D List of data classes
E List of recipients
SECTION I: Audit of Processing

1.1 The audit of all processing of personal data within a department is by far the largest task that a Data Protection Co-ordinator will have to undertake and is the most important in ensuring that the University meets its obligations under the Data Protection Act 1998.

1.2 Under the Act, the University is required on an annual basis to notify the Information Commissioner of all processing of personal data undertaken by the University, and inform the Information Commissioner of any changes to such processing or any new processing during the course of the year.

1.3 The information required by the Information Commissioner includes the purposes for which data is being processed, the data subjects about whom personal data is held, the classes of data held, recipients of that data and details of transfers of data overseas. While this information can be reported to the Information Commissioner in a summarised form for the University as a whole, an audit of all processing within the University is necessary to ensure that the notification is complete and accurate.

1.4 The University is also required to ensure that all processing of personal data is compliant with the provisions of the Act and to be able to provide evidence of compliance. A further purpose of the audit process is to verify that the processing complies with each of the Eight Principles of Data Protection and to provide such evidence.

1.5 Overall, the purposes of the audit are:

   a) to provide details of processing for notification to the Information Commissioner;
   b) to identify areas where action needs to be taken to ensure compliance;
   c) to provide information to assist in responding to requests from data subjects for access to their personal data held by the University.

1.6 Although it is not necessary to notify the Information Commissioner of the processing of personal data held in manual form, such processing will still need to be audited to ensure compliance and to assist in responding to data subject access requests.

1.7 It is not intended that miscellaneous letters and e-mails held on computer should be included in the audit process. However, it should be noted that data subjects do have the right to access personal data contained within such documents. Each department should therefore have a policy with respect to management of these documents that will ensure compliance and assist in the retrieval of personal data where necessary.

1.8 The audit of processing must be carried out on an annual basis. The Data Protection Officer must also be informed of any changes or additions to processing during the intervening period.

1.9 Where the audit indicates a possible failure to comply with the legislation, the matter should be first raised with the member of staff responsible for the data and, where
feasible, appropriate remedial action taken immediately. Details of both the failure to comply and the action taken should be recorded on the audit form.

1.10 The audit forms should be passed to the Head of Department for authorisation before being sent to the Data Protection Officer. Copies of the audit will be retained by both the department and the Data Protection Officer.

SECTION II: Audit Procedure

1. Scope of the audit

All personal data held in electronic format or contained within a structured manual filing system must be audited.

In particular, but not exclusively, the audit will cover personal data held in the following systems and formats:

- Computer databases;
- Document management systems (including documents stored in standard directory structures provided by such facilities as CFS);
- Individual computer files where appropriate eg. spreadsheets and other such analysis tools, word-processed lists;
- Structured e-mail directories;
- Structured manual filing systems that can be referenced by individual e.g. Student files, staff files, survey data forms, examination scripts, holiday charts/lists, directories, publication lists;
- Web-pages
- Photographs
- Microfiche
- Video/audio recordings
- Tissue samples

1.3 Please note that in conducting the audit it will be necessary to meet with all staff within the department to ensure that all processing of personal data is covered.

2. Frequency of audit

Departments must conduct an audit on an annual basis. After the initial audit, subsequent audits should require only the amendment of previous audit details.

Between each audit any changes in processing (additions, deletions and amendments) must be notified to the Data Protection Officer.

3. The Audit Process

For each collection of data an Audit Form must be completed. The form is in two parts. Part A requires the completion of details for notification purposes (and also for assisting in
responding to data subject access requests). Part B is a series of questions intended to highlight any areas of non-compliance. A copy of the form is given in Appendix A. Instructions for completing both parts of the form are given below.

**Audit Form Part A: Notification Details – Instructions for completion**

All parts must be completed – do not leave blanks. If something is not applicable, or if the information is not available or not known, please indicate this on the form.

**Department:** Enter department name and sub-department or division where appropriate.

**Data Collection Name:** Enter the name of the collection by which it is known in the department or other reference.

**Description:** Enter a brief description of the data collection.

**Data Owner:** Enter the name and position of the person within the department with responsibility for management and control of the data.

**Contact details:** Enter contact details for the Data Owner.

**Location of data:** Specify the locations where the data is held. If held on computer please specify the location of the computer equipment.

**Data Formats:** Tick the formats in which the data are held.

**Purpose for processing:** Select one of the purpose codes as described in Appendix B for processing the personal data held in the data collection. If none are appropriate please describe the purpose for processing.

**Data subjects:** A data subject is an individual about whom data are held. Select one or more of the data subject codes as described in Appendix C. For data subjects not covered by this list please enter a description.

**Data Classes:** Data classes are the types of personal data which are being or which are to be processed. Select all relevant data class codes as described in Appendix D. For classes of data not covered by this list please enter a description. Please note that codes C206 to C213 all refer to sensitive personal data as defined within the Act.

**Sources of personal data:** Indicate whether the personal data are obtained from the data subject or from a third-party. If a third-party please enter a description.

**Recipients of personal data:** Recipients are individuals or organisations to whom the University intends or may wish to disclose data. It does not include any person to whom the University may be required by law to disclose in any particular case, for example if required by the police under a warrant. Select all recipient codes as described in Appendix E. For recipients of data not covered by this list please enter a description.
Transfer of personal data overseas: Indicate whether personal data are transferred outside the European Economic Area (EEA)\(^1\). The choices are:

None outside the EEA
Worldwide
Name individual countries outside the EEA (if there are more than 10 countries indicate ‘Worldwide’.)

A transfer is not defined in the Act. However, the ordinary meaning of the word is transmission from one place, person, etc to another. This will include posting information on a website which can be accessed from overseas. In these circumstances it would be appropriate to indicate ‘worldwide’.

3.2.14 Processing of data by third parties: Please specify any contractors or organisations that process any of the data on behalf of the University or have direct access to the data in the course of their work for the University.

Audit Form Part B: Compliance Details – Instructions for completion

All parts must be completed – do not leave blanks. If something is not applicable, or if the information is not available or not known, please indicate this on the form.

To ensure the processing complies with the requirements of the Data Protection Act tick Yes or No in response to the following questions. If not applicable, please indicate.

The questions relate to the Principles of Data Protection as indicated below.

Fair and lawful processing (First Principle)

Q1 Has the data subject been informed of the processing?
Q2 Has the data subject been informed of the people or organisations their data may be passed onto?
Q3 Has the data subject given their consent to the processing?
Q4 If the data subject has not given their consent, can the processing be justified on the basis of necessity (see Schedules 2 and 3 of the Act in Appendix 6.3 of the Data Protection Code of Practice for definitions of necessary processing)?
Q5 If the data collection includes sensitive data (data classes C206 –C213) has the data subject given their explicit consent to process such data?

Lawful, clear and specific purposes (Second Principle)

Q6 Is the processing of the data legal?

---

\(^1\) At the time of publication the countries in the EEA are the 27 EU members states plus Norway, Liechtenstein and Iceland. Switzerland is considered to have adequate data protection controls.
The legality of the processing must not be in question. For example, it is unlawful to use a person’s National Insurance number as a personal identifier.

Q7 Has it been made clear to the data subject what the data will be used for?

Q8 Have any ‘non-obvious’ uses of the data been made clear to the data subject, i.e. things that the data subject would not have realised you were doing from a general description of the processing?

Adequate and minimum necessary data (Third Principle)

Q9 Is there a clear reason for processing each item of data?

Q10 Has it been verified that the same outcome could not be achieved, safely and effectively, with less data?

Q11 Where information is collected on a form, does it indicate to the data subject that information which is essential and that which is voluntary to give?

Q12 Is the information that is being processed adequate for the purpose? For example, if information is collected with the intention of using it later to prove the identity of individuals, a first and last name may not be enough.

Q13 Is the information that is being processed no more than is necessary? For example, in collecting information for identification purposes it may be excessive to request a person’s last three addresses.

Accuracy of data (Fourth Principle)

Q14 Have steps been taken to ensure the accuracy of the data?

Q15 Is there a system of rolling reviews of data to keep the data up to date?

[Note: if data is inaccurate or out of date it would not only breach the fourth Principle, but it could breach the third as well, because the data might not be adequate for the purpose.]

Retention of data (Fifth Principle)

Q16 Are the data being kept for no longer than is necessary to comply with relevant laws and regulations that define minimum periods of retention? (See the University’s Data Protection Code of Practice)

Q17 If data are being kept for periods longer than the legal minimum is there a good reason for doing so?

Q18 Are files periodically ‘weeded’ of irrelevant data?

Q19 Is there a clear justification for the length of time the data are retained?

Q20 Can it be confirmed that data are not being kept on a ‘just in case’ basis?

The data subject’s rights (Sixth Principle)
Q21 Does the data subject know that their personal data are being processed?
Q22 Does the data subject know why their personal data are being processed?
Q23 Does the data subject know how their personal data are being processed?
Q24 Has the data subject been informed of their rights of access?

**Appropriate security measures (Seventh Principle)**

Q25 Is the level of security adopted appropriate to the risks represented by the processing and the nature of the data to be protected?

Consideration should be given to the measures taken to guard against theft, malicious damage or corruption (including computer viruses), unlawful access, accidental disclosure, loss and destruction. Particular consideration should be given to the security of sensitive data.

Q26 Are there clear lines of responsibility for the processing operations?

Q27 Are staff who deal with personal data aware of the purposes for which it has been collected?

Q28 Are staff who deal with personal data aware of the parties to whom they can legitimately disclose the data?

Q29 Are non-University personnel and students who handle personal data aware of their responsibilities and obligations under the Data Protection Act?

Q30 Are non-University personnel and students who handle personal data adequately supervised?

Q31 Where consultants/contractors have access to or process the data, is there a data protection statement in place in the contract setting out their obligations with regard to the security and use of data? e.g. Computer service engineers, mailing houses.

Q32 Are appropriate measures in place for the secure disposal and/or destruction of personal data that are no longer required? (Please refer to the Data Protection Code of Practice for details of appropriate measures)

**Transferring personal data overseas (Eighth Principle)**

Q33 Where applicable, has the consent of the data subject been obtained to transfer personal data to countries outside the EEA which are not designated as ‘adequate’ by the Information Commissioner?

**Other Legislative and Regulatory Requirements**

Q34 To the best of your knowledge has it been determined whether any other legal or regulatory conditions apply to the processing of the personal data?
Where such conditions apply please state the applicable legislation and/or regulations.

Where such other conditions apply, are appropriate procedures and controls in place to ensure compliance?

A ‘No’ response to any of the above questions may indicate a failure to comply with the requirements of the Data Protection Act. All such responses should be discussed with the Data Owner and action agreed as necessary. If there is any doubt regarding the need for action or the type of action to be taken, the matter should be discussed with the Data Protection Officer.

Any agreed actions should be noted on the audit form. The Data Protection Co-ordinator should confirm at a later date that all agreed actions have been undertaken.

Upon completion of Parts A and B of the form the Data Protection Co-ordinator should sign the form as Auditor and then pass the form to the Head of Department for review and signature, before sending to the Data Protection Officer for recording centrally.

The forms will be reviewed by the Data Protection Officer and any issues followed up with the Data Protection Co-ordinator where necessary.

A copy of the form will be returned to the Data Protection Co-ordinator with an internal reference number added.

4. Reporting new processing or changes in processing

During the period between each audit, any new processing should be notified to the Data Protection Officer using the standard Audit Form.

New processing must clearly comply with the requirements of the Data Protection Act and must be notified to the Data Protection Officer before such processing is undertaken.

Any changes to existing processing should be notified by signed memorandum to the Data Protection Officer indicating the nature of the change and quoting the internal reference number specified on the Audit Form.
### University of Leicester

**Date Protection Audit Form**  
**Part A - Notification**

(All parts must be completed - do not leave blanks. If something is not applicable, or if the information is not available or not known, please indicate this on the form)

<table>
<thead>
<tr>
<th>Department</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Sub Dept./Division</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Data Collection Name</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Data Owner</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Position</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Contact details</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Locations of data</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Data Formats</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

- Computer
- Photograph
- Tissue
- Paper
- Video
- Other
- Microfiche
- Audio
  (please specify)

<table>
<thead>
<tr>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Data Subjects</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

- S100 - Staff including volunteers, agents, temporary and casual workers
- S101 - Customers and Clients
- S102 - Suppliers
- S103 - Members or supporters
- S104 - Complainants, correspondents and enquirers
- S105 - Relatives, guardians and associates of the data subject
- S106 - Advisers, consultants and other professional experts
- S107 - Patients
- S108 - Students
- S109 - Offenders & suspected offenders
- Other - please specify

<table>
<thead>
<tr>
<th>Data Classes</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

- C200 - Personal details
- C201 - Family, lifestyle, social circumstances
- C202 - Education & training
- C203 - Employment details
- C204 - Financial details
- C205 - Goods or services provided
- C206 - Racial or ethnic origin
- C207 - Political opinions
- C208 - Religious or similar beliefs
- C209 - Trade union membership
- C210 - Physical or mental health or condition
- C211 - Sexual life
- C212 - Offences (including alleged offences)
- C213 - Criminal proceedings, outcomes, etc.
- Other
- Other
Data sources

- Data subject
- Third-party (please specify)

Data Recipients

- R400 - Data subjects themselves
- R401 - Relatives, guardians or other persons associated with the Data subject
- R402 - Current, past or prospective employers of the Data subject
- R403 - Healthcare, social and welfare advisers or practitioners
- R404 - Education, training establishments and examining bodies
- R405 - Business associates and other professional advisers
- R406 - Employees and agents of the Data controller
- R407 - Other companies in the same group as the Data controller
- R408 - Suppliers, providers of goods or services
- R409 - Persons making an enquiry or complaint
- R410 - Financial organisations and advisers
- R411 - Credit reference agencies
- R412 - Debt collection and tracing agencies
- R413 - Survey and research organisations
- R414 - Traders in personal Data
- R415 - Trade, employer associations and professional bodies
- R416 - Police forces
- R417 - Private investigators
- R418 - Local government
- R419 - Central government
- R420 - Voluntary and charitable organisations
- R421 - Political organisations
- R422 - Religious organisations
- R423 - Ombudsmen and regulatory authorities
- R424 - The media
- R425 - Data processors
- Other - please specify

Transfers Overseas

- None outside the EEA
- Worldwide
- Countries outside EEA (please name - if greater than 10 specify worldwide)

Processing of data by third parties (please specify)
### Part B - Compliance

#### Fair and lawful processing (First Principle)

<table>
<thead>
<tr>
<th>Q1</th>
<th>Has the data subject been informed of the processing?</th>
<th>Yes</th>
<th>No</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Q2</td>
<td>Has the data subject been informed of the people or organisations their data may be passed onto?</td>
<td>Yes</td>
<td>No</td>
<td>N/A</td>
</tr>
<tr>
<td>Q3</td>
<td>Has the data subject given their consent to the processing?</td>
<td>Yes</td>
<td>No</td>
<td>N/A</td>
</tr>
<tr>
<td>Q4</td>
<td>If the data subject has not given their consent, can the processing be justified on the basis of necessity (see Schedules 2 and 3 of the Act in Appendix 6.3 of the Data Protection Code of Practice for definitions of necessary processing)?</td>
<td>Yes</td>
<td>No</td>
<td>N/A</td>
</tr>
<tr>
<td>Q5</td>
<td>If the data collection includes sensitive data (data classes C206 -C213) has the data subject given their explicit consent to process such data?</td>
<td>Yes</td>
<td>No</td>
<td>N/A</td>
</tr>
</tbody>
</table>

#### Lawful, clear and specific purposes (Second Principle)

<table>
<thead>
<tr>
<th>Q6</th>
<th>Is the processing of the data legal?</th>
<th>Yes</th>
<th>No</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Q7</td>
<td>Has it been made clear to the data subject what the data will be used for?</td>
<td>Yes</td>
<td>No</td>
<td>N/A</td>
</tr>
<tr>
<td>Q8</td>
<td>Have any 'non-obvious' uses of the data been made clear to the data subject, i.e. things that the data subject would not have realised you were doing from a general description of the processing?</td>
<td>Yes</td>
<td>No</td>
<td>N/A</td>
</tr>
</tbody>
</table>

#### Adequate and minimum necessary data (Third Principle)

<table>
<thead>
<tr>
<th>Q9</th>
<th>Is there a clear reason for processing each item of data?</th>
<th>Yes</th>
<th>No</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Q10</td>
<td>Has it been verified that the same outcome could not be achieved, safely and effectively, with less data?</td>
<td>Yes</td>
<td>No</td>
<td>N/A</td>
</tr>
<tr>
<td>Q11</td>
<td>Where information is collected on a form, does it indicate to the data subject that information which is essential and that which is voluntary to give?</td>
<td>Yes</td>
<td>No</td>
<td>N/A</td>
</tr>
<tr>
<td>Q12</td>
<td>Is the information that is being processed adequate for the purpose?</td>
<td>Yes</td>
<td>No</td>
<td>N/A</td>
</tr>
<tr>
<td>Q13</td>
<td>Is the information that is being processed no more than is necessary?</td>
<td>Yes</td>
<td>No</td>
<td>N/A</td>
</tr>
</tbody>
</table>

#### Accuracy of data (Fourth Principle)

<table>
<thead>
<tr>
<th>Q14</th>
<th>Have steps been taken to ensure the accuracy of the data?</th>
<th>Yes</th>
<th>No</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Q15</td>
<td>Is there a system of rolling reviews of data to keep the data up to date?</td>
<td>Yes</td>
<td>No</td>
<td>N/A</td>
</tr>
</tbody>
</table>

#### Retention of data (Fifth Principle)

<table>
<thead>
<tr>
<th>Q16</th>
<th>Are the data being kept for no longer than is necessary to comply with relevant laws and regulations that define minimum periods of retention? (See the Data Protection Code of Practice)</th>
<th>Yes</th>
<th>No</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Q17</td>
<td>If data are being kept for periods longer than the legal minimum is there a good reason for doing so?</td>
<td>Yes</td>
<td>No</td>
<td>N/A</td>
</tr>
</tbody>
</table>
Q18 Are files periodically 'weeded' of irrelevant data?  
Q19 Is there a clear justification for the length of time the data are retained?  
Q20 Can it be confirmed that data are not being kept on a 'just in case' basis?  

The data subject's rights (Sixth Principle)  
Q21 Does the data subject know that their personal data are being processed?  
Q22 Does the data subject know why their personal data are being processed?  
Q23 Does the data subject know how their personal data are being processed?  
Q24 Has the data subject been informed of their rights of access?  

Appropriate security measures (Seventh Principle)  
Q25 Is the level of security adopted appropriate to the risks represented by the processing and the nature of the data to be protected?  
(Consideration should be given to the measures taken to guard against theft, malicious damage or corruption (including computer viruses), unlawful access, accidental disclosure, loss and destruction.  
Q26 Are there clear lines of responsibility for the processing operations?  
Q27 Are staff who deal with personal data aware of the purposes for which it has been collected?  
Q28 Are staff who deal with personal data aware of the parties to whom they can legitimately disclose the data?  
Q29 Are non-University personnel and students who handle personal data aware of their responsibilities and obligations under the Data Protection Act?  
Q30 Are non-University personnel and students who handle personal data adequately supervised?  
Q31 Where consultants/contractors have access to or process the data, is there a data protection statement in place in the contract setting out their obligations with regard to the security and use of data?  
e.g. Computer service engineers, mailing houses.  
Q32 Are appropriate measures in place for the secure disposal and/or destruction of personal data that are no longer required?  
(Please refer to the Data Protection Code of Practice for details of appropriate measures)  

Transferring personal data overseas (Eighth Principle)  
Q33 Where applicable, has the consent of the data subject been obtained to transfer personal data to countries outside the EEA which are not designated as 'adequate' by the Information Commissioner?  

Other Legislative and Regulatory Requirements  
Q34 To the best of your knowledge has it been determined whether any other legal or regulatory conditions apply to the processing of the personal data?  
Q35 Where such conditions apply please state the applicable legislation and/or regulations.  
Q36 Where such other conditions apply, are appropriate procedures and controls in place to ensure compliance?  

Audited by:  
Authorised by:  

Date:  

Yes  No  N/A
APPENDIX B: Purposes

P001  Staff administration
Appointments or removals, pay, discipline, superannuation, work management or other personnel matters in relation to the staff of the data controller.

P002  Advertising, marketing and public relations
Advertising or marketing the data controller’s own business, activity, goods or services and promoting public relations in connection with that business or activity or those goods or services.

P003  Accounts and records
Keeping accounts relating to any business or other activity carried on by the data controller, or deciding whether to accept any person as a customer or supplier, or keeping records of purchases, sales or other transactions for the purpose of ensuring that the requisite payments and deliveries are made or services provided by him or to him in respect of those transactions, or for the purpose of making financial or management forecasts to assist him in the conduct of any such business or activity.

P004  Accounting and auditing
The provision of accounting and related services; the provision of an audit where such an audit is required by statute.

P005  Administration of justice
Internal administration and management of courts of law or tribunals and discharge of court business.

P006  Administration of membership records
The administration of membership records.

P007  Advertising marketing and public relations for others
Public relations work, advertising and marketing, including host mailings for other organisations and list broking.

P008  Assessment and collection of taxes and other revenue
Assessment and collection of taxes, duties, levies and other revenue. You will be asked to indicate the type of tax or other revenue concerned.

P009  Benefits, grants and loans administration
The administration of welfare and other benefits. You will be asked to indicate the type(s) of benefit you are administering.

P012  Consultancy and advisory services
Giving advice or rendering professional services. The provision of services of an advisory, consultancy or intermediary nature. You will be asked to indicate the nature of the services which you provide.

P014  Crime prevention and prosecution of offenders
Crime prevention and detection and the apprehension and prosecution of offenders. This includes the use of most CCTV systems which are used for this purpose.
**P015  Debt administration and factoring**
The tracing of consumer and commercial debtors and the collection on behalf of creditors. The purchasing of consumer or trade debts, including rentals and instalment credit payments, from business.

**P016  Education**
The provision of education or training as a primary function or as a business activity.

**P017  Fundraising**
Fundraising in support of the objectives of the data controller.

**P018  Health administration and services**
The provision and administration of patient care.

**P019  Information and databank administration**
Maintenance of information or databanks as a reference tool or general resource. This includes catalogues, lists, directories and bibliographic databases.

**P021  Journalism and media**
Processing by the data controller of any journalistic, literary or artistic material made or intended to be made available to the public or any section of the public.

**P022  Legal services**
The provision of legal services, including advising and acting on behalf of clients.

**P023  Licensing and registration**
The administration of licensing or maintenance of official registers.

**P024  Pastoral care**
The administration of pastoral care by a vicar or other minister of religion.

**P025  Pensions administration**
The administration of funded pensions or superannuation schemes. Data controllers using this purpose will usually be the trustees of pension funds.

**P027  Private investigation**
The provision on a commercial basis of investigatory services according to instruction given by clients.

**P028  Processing for not for profit organisations**
Establishing or maintaining membership of or support for a body or association which is not established or conducted for profit, or providing or administering activities for individuals who are either members of the body or association or have regular contact with it.

**P029  Property management**
The management and administration of land, property and residential property and the estate management of other organisations.
P030  **Provision of financial services and advice**  
The provision of services as an intermediary in respect of any financial transactions including mortgage and insurance broking.

P031  **Realising the objectives of a charitable organisation or voluntary body**  
The provision of goods and services in order to realise the objectives of the charity or voluntary body.

P032  **Research**  
Research in any field, including market, health, lifestyle, scientific or technical research. You will be asked to indicate the nature of the research undertaken.

P033  **Trading/sharing in personal information**  
The sale, hire, exchange or disclosure of personal data to third parties in return for goods / services / benefit.
APPENDIX C: Data Subjects

S100 - Staff including volunteers, agents, temporary and casual workers
S101 - Customers and clients
S102 - Suppliers
S103 - Members or supporters
S104 - Complainants, correspondents and enquirers
S105 - Relatives, guardians and associates of the data subject
S106 - Advisers, consultants and other professional experts
S107 - Patients
S108 - Students and pupils
S109 - Offenders and suspected offenders

All of the above categories include current, past or prospective data subjects.
APPENDIX D: Data Classes

C200 Personal details
Included in this category are classes of data which identify the data subject and their personal characteristics. Examples are names, addresses, contact details, age, sex, date of birth, physical descriptions, identifiers issued by public bodies, eg NI number.

C201 Family, lifestyle and social circumstances
Included in this category are any matters relating to the family of the data subject and the data subject’s lifestyle and social circumstances. Examples are details about current marriage and partnerships and marital history, details of family and other household members, habits, housing, travel details, leisure activities, membership of charitable or voluntary organisations.

C202 Education and training details
Included in this category are any matters which relate to the education and any professional training of the data subject. Examples are academic records, qualifications, skills, training records, professional expertise, student and pupil records.

C203 Employment details
Included in this category are any matters relating to the employment of the data subject. Examples are employment and career history, recruitment and termination details, attendance record, health and safety records, performance appraisals, training records, security records.

C204 Financial details
Included in this category are any matters relating to the financial affairs of the data subject. Examples are income, salary, assets and investments, payments, creditworthiness, loans, benefits, grants, insurance details, pension information.

C205 Goods or services provided
Included in this category are classes of data relating to goods and services which have been provided. Examples are details of the goods or services supplied, licences issued, agreements and contracts.

C206 Racial or ethnic origin
C207 Political opinions
C208 Religious or other beliefs of a similar nature
C209 Trade union membership
C210 Physical or mental health or condition
C211 Sexual Life
C212 Offences (including alleged offences)
C213 Criminal proceedings, outcomes and sentences
APPENDIX E: Recipients

R400 - Data subjects themselves
R401 - Relatives, guardians or other persons associated with the data subject
R402 - Current, past or prospective employers of the data subject
R403 - Healthcare, social and welfare advisers or practitioners
R404 - Education, training establishments and examining bodies
R405 - Business associates and other professional advisers
R406 - Employees and agents of the data controller
R407 - Other companies in the same group as the data controller
R408 - Suppliers, providers of goods or services
R409 - Persons making an enquiry or complaint
R410 - Financial organisations and advisers
R411 - Credit reference agencies
R412 - Debt collection and tracing agencies
R413 - Survey and research organisations
R414 - Traders in personal data
R415 - Trade, employer associations and professional bodies
R416 - Police forces
R417 - Private investigators
R418 - Local government
R419 - Central government
R420 - Voluntary and charitable organisations
R421 - Political organisations
R422 - Religious organisations
R423 - Ombudsmen and regulatory authorities
R424 - The media
R425 - Data processors