# University data protection code: collection and use of staff personal and sensitive personal data

<table>
<thead>
<tr>
<th>Author</th>
<th>Associate Chief Information Officer (Information Assurance &amp; Governance)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Approved by</td>
<td>Principal’s Office</td>
</tr>
<tr>
<td>Approval date(s)</td>
<td>August 2013</td>
</tr>
<tr>
<td>Review date</td>
<td>May 2016</td>
</tr>
<tr>
<td>Version</td>
<td>1.0</td>
</tr>
<tr>
<td>Document type</td>
<td>Policy</td>
</tr>
<tr>
<td>Activity/Task</td>
<td>Information governance and security</td>
</tr>
<tr>
<td>Keywords</td>
<td>[Insert_Keywords]</td>
</tr>
<tr>
<td>Document location</td>
<td>[Insert_Saved_location]</td>
</tr>
<tr>
<td>Confidentiality</td>
<td>PUBLIC</td>
</tr>
<tr>
<td>Version Number</td>
<td>Purpose / Changes</td>
</tr>
<tr>
<td>----------------</td>
<td>----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>0.1</td>
<td>Final draft for presentation for peer review and approval – based on earlier approved Code on the collection and use of student personal and sensitive personal data</td>
</tr>
<tr>
<td>0.2</td>
<td>Revisions from the University Chief Information Officer incorporated</td>
</tr>
<tr>
<td>0.3</td>
<td>Revisions from the Head of Human Resources incorporated</td>
</tr>
<tr>
<td>0.4</td>
<td>Revised following review by Principal’s Office</td>
</tr>
<tr>
<td>0.5</td>
<td>Revised following discussions at HR Services and staff representative groups (25-July-2013)</td>
</tr>
<tr>
<td>1.0</td>
<td>Changes made following Union consultation – Code now finalised</td>
</tr>
<tr>
<td>1.1</td>
<td>Minor amendments made to clarify where personal data is processed in relation to assessment of research outputs e.g. REF, health &amp; safety activities, public safety &amp; crime prevention and internal or external audit</td>
</tr>
</tbody>
</table>
Contents
Purpose ............................................................................................................................................ 4
Scope .................................................................................................................................................. 4
The University of St Andrews as a Data Controller ...................................................................... 5
Personal and sensitive personal data ............................................................................................... 5
The conditions legitimising the processing of personal data of members of staff ....................... 5
The conditions legitimising the processing of personal data of former members of staff ............ 7
How will the University use your personal data ............................................................................ 8
Transfer of personal data to third parties ....................................................................................... 9
The conditions legitimising the processing of sensitive personal data of staff ............................. 12
The data protection principles ........................................................................................................... 15
Revision of the Code ....................................................................................................................... 17
Availability ..................................................................................................................................... 17
Contacts, further information .......................................................................................................... 18
Purpose

The protection of personal information collected and processed by the University is legislated through the European Directive 95/46/EC the protection of individuals with regard to the processing of personal data (“the Directive”) which gave rise to an Act of the United Kingdom Parliament: the Data Protection Act 1998 (“the DPA”). The University takes its obligations to protect personal information and to uphold the rights and freedoms of individuals seriously.

One of the core principles of data protection legislation is that personal data is processed fairly. Fairly, in this context, is concerned with individuals being informed at the point of data collection how their personal information will be used by the organisation that has collected that information.

The purpose of this statement is therefore to inform members of staff how their personal information will be used. This statement is not exhaustive: it does not detail all of the uses that the University may reasonably make of the personal data of employees. The statement aims to set a reasonable expectation amongst individuals as to how the University will use and manage their personal information during their time at the University and following their departure.

The statement is also is intended to support University initiatives to improve the quality of the staff experience: where there is a reasonable expectation amongst members of staff that their personal data may be used by the University.

Scope

This Code:

- Sets out the University’s obligations as a data controller;
- Provides an insight into the conditions, prescribed by law, through which the University can make use of your personal data – detailing why it is not always necessary for the University to seek consent to process personal information;
- Provides an overview as to how your personal data will be used;
- Sets out the limited conditions under which your personal data may be made available to a third party;
- Provides an insight into the conditions, prescribed by law, through which the University can make use of your sensitive personal data; and
- Explains how the University manages your personal and sensitive personal data in line with the data protection principles.
The University of St Andrews as a Data Controller

The University of St Andrews is registered as a data controller with the Information Commissioner’s Office ("the ICO") (the ICO being the UK supervisory authority responsible for oversight of the DPA and the enforcement of that Act). As a data controller the University is required to confirm with the ICO annually (in general terms) the purposes for which it processes personal data and sensitive personal data, and which persons are affected by such processing.

The ICO maintains a public register of data controllers, so that individuals can ascertain what personal information is being processed by a particular data controller. The University’s registration number in this regard is Z5909128. To fully understand what personal data the University holds and processes, you may wish to consult both this statement and the University’s entry within the ICO data protection register. That, and the register, are available on-line from www.ico.gov.uk

Personal and sensitive personal data

The DPA is concerned with the use made of personal and sensitive personal data. In broad terms, personal data is information (held electronically or in a structured form, e.g. within a recognised filing system) that relates to a living individual in a significant biographical sense, i.e. the information reveals something about the life of that person. Sensitive personal data is more clearly defined as data consisting of information regarding:

1. Racial or ethnic origins of an individual;
2. Political opinions;
3. Religious beliefs or beliefs of a similar nature;
4. Trade union membership;
5. A person’s physical or mental health condition;
6. Their sexual life;
7. Details of any proceedings for any offence committed or alleged to have been committed by the data subject, the disposal of such proceedings or the sentence of any court in such proceedings; and
8. Outcomes of criminal convictions.

The DPA sets out the conditions which must be present before the University can make use of your personal and sensitive personal data. These are briefly outlined below.

The conditions legitimising the processing of personal data of members of staff

The most common conditions that the University will rely upon for the lawful processing of the personal data of staff are outlined below.

- Processing for the performance of a contract (between the member of staff and the University)
The majority of the personal information that the University collects from both prospective employees and members of staff is used by it so that it can provide access to a range of services and facilities that are consistent with supporting the contract of employment. The relevant conditions for processing of personal data in these circumstances are found in SCHEDULE 2, paragraphs 2(a) and (b) of the DPA i.e.

“The processing is necessary-

(a) for the performance of a contract to which the data subject [a member of staff] is party, or

(b) for taking steps at the request of the data subject [a prospective employee] with a view to entering into a contract [of employment at the University]”

On accepting an offer of employment, the University will ask for bank details so that salary and other payments can be made. The use of those details is consistent with the University meeting its contractual obligations (payment). In that instance the University is processing that information as per the condition available at SCHEDULE 2 paragraph 2(a) of the DPA.

- **The processing is necessary for compliance with legal obligations other than a contract [to which the University is subject]**

In prescribed circumstances the University is required by law to make available to other agencies and authorities personal information concerning its members of staff [SCHEDULE 2, paragraph 3]. Examples include statutory returns to HMRC.

- **The processing is necessary to protect the vital interests [of members of staff]**

Vital interests in this context mean protecting the life and wellbeing of an individual or protecting an individual’s property from serious and substantial damage. For example, the University would inform the emergency services of known medical conditions of a staff member where they had lost consciousness. See SCHEDULE 2, paragraph 4 of the DPA.

- **The processing is necessary for the legitimate interests pursued by the University or by third parties who may seek disclosure – except where that processing would prejudice the rights and freedoms of members of staff**

The relevant condition here is available from SCHEDULE 2, paragraph 6(1) of the DPA. The University can be asked to release personal data to a third party and it would only do so subject to satisfying the relevant conditions within the DPA. This will involve a balancing exercise to determine whether the third party has a legitimate interest in having access to the personal data in question and establishing if release would be unfair to the person(s) concerned. For example the University will disclose to the University and Colleges Union (UCU) names and contact details of members of staff who have just joined the University so that the UCU can then promote a range of services to those persons. Such a transfer is in the legitimate interests of the third party (the UCU) and would not be harmful to the members of staff concerned.
• Consent is given to process personal data

Circumstances may arise where it will be necessary for the University to seek the consent of members of staff so that it can process that personal data. However, this is likely to be a relatively rare occurrence, as the majority of the information processed by the University is done for fulfilling contractual purposes (see above). Where it is necessary to seek consent to process their personal data, this will be made clear to individuals at the point of data collection. Consent is optional. Individuals are under no compulsion to provide their consent. The relevant condition here is available from the DPA, SCHEDULE 2, paragraph 1.

For the avoidance of doubt when signing to accept the terms and conditions of employment the University is not asking members of staff for their consent to process personal data.

The conditions legitimising the processing of personal data of former members of staff

As a public body, the University has a number of obligations that will require it to process personal data of individuals after they have left, i.e. where there is no longer a contract in place between an individual and the University. In those circumstances, the University is likely to call upon the condition available in SCHEDULE 2, paragraph 6(1) of the DPA (see above), although depending on the circumstances other SCHEDULE 2 conditions may be appropriate.
How will the University use your personal data

All personal data held by the University – for which it has responsibility as a data controller – will be processed as per the provisions of the legislation referred to above, i.e. the Directive and the DPA. This information may be held by the University in electronic or paper form, and may be used for activities such as:

- **Managing the contract of employment**
  - i. The administering of applications to work at the University.
  - ii. The creation and maintenance of a staff record – this can include maintaining records on sickness absence.
  - iii. Administering salary and pension payments, annual leave entitlement etc.
  - iv. Administering access to services and facilities provided by or through the University as necessary to support your employment and time spent with the University, e.g. access to Library lending facilities, ICT account creation and provision for e-mail services, production of a staff ID card, access control to buildings and/or facilities. This will include face-to-face and on-line services and facilities.

- **v. Communication**
  - a. The University will hold and make use of home and other contact details to attempt to reach individuals as necessary to support day-to-day operations and to maintain the health, safety and wellbeing of the University community, specifically:
    - i. It will make those personal data available to other members of staff and/or agents of the University to enable persons to be contacted for the purposes of disaster recovery or business continuity
  - b. The University will also make use of work-based contact details to enable individuals who engage with the University or any of its agents to make contact with you in connection with your role at St Andrews and/or to alert you to the services and facilities available to you as a member of staff.

- **vi.** The administration and execution of voluntary surveys of staff opinion – connected with the assessment and development of the staff experience and performance of the University.

- **vii.** The organisation and delivery of training/staff development activities both at the University and in any other institution with which the University engages for providing such development.

- **viii.** Performance appraisals and review, including assessment of research outputs e.g. REF.

- **ix.** The administration and execution of all processes/procedures concerning:
  - a. Complaints;
  - b. Appeals (academic and non-academic); and
  - c. Staff discipline.
The provision of staff support services

i. The administration and provision of welfare and pastoral services. This could include professional counselling services provided by or through the University.

ii. Careers guidance.

iii. The admission and provision of health care services provided by or through the University.

The management of the University – including the University meeting any legal and/or regulatory obligations

i. Statistical processing (compilation, monitoring and dissemination internally and externally to agencies to whom the University has an obligation to report, such as funding bodies).

ii. Equal opportunities monitoring by the University or by external agencies which the University has an obligation to assist, such as funding bodies.

iii. Planning for and undertaking health and safety activities.

iv. Retention of monies paid and the dissemination of such information to such agencies (e.g. HMRC) as prescribed by law.

Public safety and the prevention and detection of crime

i. Images captured by Closed Circuit Television (CCTV) systems operated by or on behalf of the University will be used for purposes of providing a safe campus environment and for the prevention and detection of crime.

ii. Data from the University access control systems, network log-files and vehicle trackers may be used to understand or determine whether an individual was in a particular location or making use of a particular resource at a point in time. Such information may be used to support investigations regarding whether University Policy and/or Regulation have been breached and/or for the detection of crime.

The maintenance of the University archive

i. Core elements of the staff record will be held in perpetuity within the University archive (both physical and electronic). Such information will be used to develop and sustain the institution’s corporate memory. This will assist the University in its corporate decision-making and in meeting its wider societal obligations, such as the provision of references, or developing an understanding of the composition of the staff body over time.

The above is not intended to be an exhaustive list.

Transfer of personal data to third parties

Partner educational/research establishments

The University will transfer personal data of members of staff who work with partnering institutions as necessary to manage and administer that individual’s work with that body.
• **Next of kin**

Under normal circumstances the University will not disclose any personal data of members of staff to their next of kin without their consent. The University may, however, contact a member of staff to inform them that another party wishes to make contact.

Where a member of staff has left the University for whatever reason, or they are not in attendance (e.g. on leave of absence) and a third party makes enquiries about them, or seeks to contact them, the University may (as a last resort) confirm with that party that it is unable to assist the enquirer, where the University cannot contact the individual concerned. Stating that the University cannot provide any such assistance will in itself confirm that an individual is not in attendance at the University. However, the reasons for non-attendance will not be disclosed.

• **Where the vital interests of a member of staff or another person are threatened**

The University may disclose the personal data and sensitive personal data of a member of staff to those third parties noted above and other relevant third parties such as the police and/or health care professionals, *without prior consent and/or notification*, where it is necessary for the University to act to protect the vital interests of that individual or another person(s). Vital interests in this context take the meaning as per that provided within Recital 31 of the (Data Protection) Directive, i.e. the release of information that is “essential for the data subject’s life.” This will also include the vital interest of other parties. Thus, passing details of a member of staff’s physical or mental health condition to health care professionals and/or the police where there is an emergency medical situation that threatens or is likely to threaten a person’s life is permissible under law. This may include the passing of information made available to the University under confidence by a member of staff, such as during a period of counselling. TheUniversity will also normally confirm with the police and/or other authorities the details of a member of staff’s next of kin. The University may also take steps to notify next of kin where an individual has developed a life threatening condition and is unable to do so themselves.

The University may also make available to health care professionals details of a member of staff’s religious belief and information concerning racial or ethnic origin where that information may have a bearing on the ability of a health care authority to protect the vital interests of that person.

Vital interests could also extend to situations whereby serious or substantial damage to an individual’s property has occurred or may occur. Therefore, the University may pass information to the police where it believes that a member of staff is likely to cause substantial damage to another person’s property.

Health care professionals are defined in a number of UK Acts of Parliament and typically include registered medical practitioners, registered nurses, midwives, health visitors and clinical psychologists.
• **The Police and other relevant authorities**

The University may pass to the police and other relevant authorities information necessary to assist that party in the purposes of the:

- Prevention and detection of crime;
- Apprehension and prosecution of offenders; and
- Assessment or collection of any tax or duty or imposition of a similar nature.

Prior to the release of personal and/or sensitive personal data to the police or a relevant authority, the University will first satisfy itself that the request for information is legitimate and that the disclosure of the information is lawful. In this regard, the University will make reference to the provisions of the DPA provided for in sections 28 and 29 and SCHEDULES 2 and 3 as appropriate. If the University finds the request to be unlawful, then the information requested will be withheld, and only released should a Court Order be served upon the University. A record of the decision to disclose or to decline the request will be made, and the decision to disclose the requested information will be restricted to those identified in the corresponding University policy concerning transfer of information to a third-party for the purposes of crime detection and prevention.

• **Recognised Trade Unions**

The University may pass on to recognised trade unions details of individuals who have recently taken up employment with the University, so that a trade union may make initial contact to inform individuals about the services provided by them.

• **References**

The University may release personal information concerning a current or former member of staff to a third party in response to a request for a reference when it has the prior consent of the individual concerned.

• **Research partners / research funders**

The University may pass personal information concerning current or former members of staff to support the application for research funding, the monitoring and/or assessment of research outputs, or to support other activities related to supporting and managing research.

• **Internal/external audit**

The University may pass personal information concerning current or former members of staff to internal or external auditor, where the information is required to support audit activities. This can include making bank details available to auditors for inspection for the purposes of fraud detection.
• **Agents of the University**

The University engages with third party contractors for the provision of services and goods. Before an agent of the University will be given access to personal data for which the University is responsible as data controller, contractual terms will exist between the University and that party which:

- Specify and limit the uses which that party can make of the personal data with which it is provided or to which it may have access through the University; and
- Establish to the University’s satisfaction that the agent has in place sufficient organisational and technical means to protect personal information made available to it against accidental loss or any form of unauthorised access and subsequent use.

• **Personal information secured by the University during disciplinary investigations and proceedings**

Information secured by the University through the course of disciplinary investigations and associated proceedings (such as witness statements) are deemed to have been provided to the University in confidence solely for the purposes of administering a disciplinary investigation and all associated processes. Insofar as University policy, regulations and procedures apply, the identity of the persons concerned and the information provided by them will be kept confidential within the confines of those proceedings, including any subsequent appeals.

Such information will not normally be released to a third party without the prior consent of the individual(s) concerned, namely the person who has supplied a witness statement, the subject(s) of that statement and any other named individuals. Circumstances can arise where a third party could attempt to seek such information through the DPA (when they seek personal data held by the University which relates to them) or through the Freedom of Information (Scotland) Act 2002 (FOISA). Such cases must be judged in terms of the application for information and the relevant legislation.

• **Debt collection agencies**

The University may provide personal details to a debt collection agency where it is necessary to seek resolution on outstanding monies owed to the University and/or the return of resources to the University.

**The conditions legitimising the processing of sensitive personal data of staff**

A data controller cannot lawfully make use of sensitive personal data unless it meets at least one of a set of eight conditions set out within SCHEDULE 3 DPA, or other conditions as established by Statutory Instruments e.g. SI 2000, No.417. In many (but not all) instances it will be necessary for the University to secure the explicit consent of the member of staff before sensitive personal data is processed.
Where the University requires the explicit consent to use sensitive personal data, the terms of use for such data will normally be notified to the member of staff at the point of data collection. In general terms the University may use sensitive personal data (without explicit consent) for the following purposes.
• To perform a right or obligation which is conferred in law on the University in connection with employment

The University may find that it is required by legislation and/or from decisions set out in case law to process sensitive personal data when that processing is connected with an employment related matter e.g. making financial returns to HMRC, retaining records of sickness absence, using records of sickness absence to ensure that an individual is not treated unfavourably.

• To protect the vital interests of a member of staff or another person

• Processing sensitive personal data where those personal data have been made public through the actions of the member of staff

The University may acknowledge in a minute of a meeting that a member of staff is a member of a trade union when they are acting in the capacity of a representative of that body.

• Where the processing is connected with any active or potential legal proceedings including obtaining legal advice

The University may process sensitive personal data in conjunction with taking or preparing to take legal action. This may include the disclosure of sensitive personal data to the University’s lawyers or other legal representative.

• Medical purposes

The University may make use of sensitive personal data for the purposes of preventative medicine, medical diagnosis, medical research, the provision of care and treatment and the management of healthcare services, where those services are provided by a [state registered] health care professional or by a professional who in the circumstances owes a duty of confidentiality which is equivalent to that which would arise if that person were a health professional.

• Equal opportunities monitoring and review

Information on racial or ethnic origin, religious belief and a physical or mental health condition(s) may be used by the University to review data on the equality of opportunity and treatment of persons.

• Disability and data protection

If a member of staff at any point prior to or during their time at University provides information about a disability which they believe themselves to have, and unless that individual explicitly records an objection with the University, the information will be passed to any University employee or agent of the University (as appropriate) for use which is consistent with:
The provision of the contract of employment;
- The provision of services to support employees; or
- The management of the University – including the University meeting any legal and/or regulatory obligations.

The data protection principles

The following sections provide a brief overview as to how personal data will be held and processed in line with each of the 8 DPA principles.

1. Personal data will be processed fairly and lawfully

The University will advise members of staff how their personal data will be used, normally at the point of data collection. This is commonly referred to as a fair collection notice. This Code assists in that process. Prospective members of staff will have sight of this Code prior to taking up employment and again once they have joined the University.

2. Personal data will only be processed for the purposes for which it was collected

The University will only make use of your personal data for the purposes for which it was collected. Those purposes are outlined within this Code, the University’s notification made to the ICO and in the fair collection notices that are presented to you at the point of data collection. If you feel that the University is not meeting this requirement, you should write to the University Associate Chief Information Officer (Information Assurance & Governance), detailing your concerns. Individuals have the right under the DPA to ask a data controller (in this instance the University) to stop processing their personal data where to do so is causing or would cause substantial damage or distress. The University has 20 days in which to respond with a decision on that matter.

3. Personal data should be adequate, relevant and not excessive in relation to the purpose(s) for processing

The University will seek to collect only the level of personal data that is required for any given purpose. Data collection processes will be reviewed at the point of development to ensure that information being requested is adequate, relevant and not excessive.

4. Accuracy of personal and sensitive personal data

The fourth data protection principle requires that the personal data held by the University “shall be accurate and, where necessary, kept up to date.” Members of staff should ensure that all personal data they provide to the University is accurate, complete and up-to-date. Staff should also notify the University of any changes in their circumstances which impact on the accuracy and completeness of their personal data, as held by the University.

5. Retention and destruction of personal and sensitive data

Personal data will be retained no longer than is necessary for the purpose(s) for which it was collected. The University will develop and maintain retention schedules for different types of
data. These will establish either the point in time at which records and the information contained within them will be destroyed, or where records are to be held in perpetuity – which information will be protected within the University archive.
6. **Personal data should be processed in accordance with the rights of data subjects as described under the Act**

These rights include:

- The right (subject to the payment of a fee) to understand what personal data is held by the University and the origin of that data, as well as to receive a copy of that information;
- The right to ask the University to stop processing personal data where to do so is or is likely to cause substantial damage or distress to them or another person;
- The right to ask the University to stop processing personal data – where that processing is concerned with direct marketing; and
- The right to insist that some decisions should not be taken by automatic means and to be informed when some decisions are made on an automatic basis.

The University will publish on its website what members of staff need to do if they wish to exercise these rights.

7. **Appropriate technical and organisational measures shall be taken to protect against unauthorised or unlawful processing of data and to protect against its accidental destruction or loss**

The University will maintain an information security policy which sets out in broad terms how the confidentiality, integrity and accessibility of both personal data and the information systems used to create and manage those data will be protected and maintained. That policy will guide the University in the development and operation of safe and secure information management practices. This will also address the training and guidance regime that will be made available to staff and agents of the University.

8. **Personal data will not be transferred to any country or territory outside the European Economic Area (EEA) unless adequate safeguards for the protection of that data are in place**

The University will not transfer personal data to a country or territory outside the EEA without first having secured the relevant protections to safeguard those data.

---

**Revision of the Code**

This Code will be reviewed at regular intervals. The review period will be approved by the University and recorded on the accompanying coversheet. Any significant change to relevant legislation, University Policy or procedures primarily concerned with the protection of personal data may trigger an earlier review. The Code will be presented to the Principal’s Office for approval.

**Availability**

This Code will be published on the University website, and copies will be provided to members of staff when they join the University.
Contacts, further information

Enquiries about this Code should be directed to the Associate Chief Information Officer (Information Assurance & Governance) or by e-mailing data-protection@st-andrews.ac.uk