University data protection code: collection and use of student personal and sensitive personal data

Author	Head of Information Assurance and Governance
Approved by	CPL Steering Group
Approval date(s)	08 August 2017
Review date	25-May-2018
Version	2.7
Document type	Policy
Activity/Task	Information governance and security
Keywords	
Document location	
Confidentiality	PUBLIC

Version Control Table

Version Number	Purpose / Changes	Author	Date
1.0	Approved by Principal's Office – no changes.		29-Aug-2012
1.1	Minor updates – management of sensitive personal data.	C Milne	09-Apr-2013
2.0	Updates provided on the basis of feedback received from Registry and Finance.	C Milne	20-May-2013
2.1	Updated to include reference to the passing of invoices to sponsors.	C Milne	30-May-2013
2.2	Updated to note that data transfers to local authorities can be made without consent for purposes of maintaining the electoral register.	C Milne	10-Oct-2013
2.3	Updated to include reference to HESA fair collection notice.	C Milne	20-May-2014
2.4	Text added into pages 9 and 12 on the transfer of information to a third party to protect the wellbeing of a student or others; to help the University meet its duty of care. Additional changes made: emergency contacts, sponsors and partner institutions following annual review exercise.	C Milne	20-Feb-2015 through 01-May-2015
2.5	HESA fair collection notice URL updated.	C Milne	08-June-2015
2.6	Minor updates made including specific reference to University making contact with students to advice of careers services and sporting facilities provided by the AU.	C Milne	11-August-2016
2.7	Minor updates made including: HESA fair collection notice details updated and use of CCTV to support investigations where it is believed that University Policy or Regulation may have been breached and legal basis for transfer of personal data to the SA for the provision of membership services.	C Milne	21-July-2017

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 students 5
The conditions legitimising the processing of personal data of former students 7
How will the University use your personal data 7
Transfer of personal data within the University 10
Transfer of personal data to third-parties 10
How will the University use your sensitive personal data 14
The conditions legitimising the processing of sensitive personal data of students 14
Mitigating circumstances 15
The data protection principles 16
Revision of the Code 17
Availability 18
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 students 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 its students. 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 student experience: where there is a reasonable expectation amongst the student body that their personal data may be used by the University. Some of these uses of that data will assist the University to improve the quality of the student experience through the development and modernisation of services.

Scope

This Code:

- Introduces 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.org.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:

a) Racial or ethnic origins of an individual;
b) Political opinions;
c) Religious beliefs or beliefs of a similar nature;
d) Trade union membership;
e) A person's physical or mental health condition;
f) Their sexual life;
g) 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
h) 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. The most common conditions that the University will rely upon for the lawful processing of the personal data of students are outlined below.

The conditions legitimising the processing of personal data of students

- Processing for the performance of a contract (between the student and the University)

  When an individual accepts an unconditional offer of study, they enter into a contract with the University of St Andrews. The majority of the personal information that the University

collects from both prospective students and matriculated students is used by it so that it can provide access to a range of educational services and facilities that are consistent with supporting that (contractual) relationship. 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 student] *is party, or*
>
> *(b) for taking steps at the request of the data subject* [a prospective student] *with a view to entering into a contract* [matriculating at the University]"

For example, when applying for a place at the University, many prospective students provide the University with a passport style photograph. The University will use that information to produce a Student ID card for that individual, so that it is ready for collection during arrivals weekend or matriculation. The University is processing that information as per the condition available at SCHEDULE 2 paragraph 2(b) of the DPA.

Following matriculation, the University could also make use of student photographs by circulating these to lecturers so that they can begin to recognise students that they will work with. The use of the photograph in that instance is consistent with the University meeting its contractual obligations (administering and providing for a high quality student experience). In that instance the University is processing that information as per the condition available at SCHEDULE 2 paragraph 2(a) of the DPA.

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

  In prescribed circumstances the University is required by law to make available to other agencies and authorities personal information concerning its students [SCHEDULE 2, paragraph 3]. For example, the Medical Act 1983 requires that proof of the qualifications of medical graduates is provided to the General Medical Council.

- <u>The processing is necessary to protect the vital interests [of students]</u>

  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 student where they had lost consciousness. See SCHEDULE 2, paragraph 4 of the DPA.

- <u>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 students</u>

  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 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.

- Consent is given to process personal data

  Circumstances will arise where it will be necessary for the University to seek the consent of students 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 and will always be truly 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 – at matriculation, when signing to accept the terms and conditions as a student of the institution, the University ***is not*** asking students for their consent to process personal data and/or sensitive personal data.

The conditions legitimising the processing of personal data of former students

As a degree awarding institution and 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 will or may be used for activities such as:

- The provision of a higher education or training
  i. The administering of applications to study at the University.
  ii. The creation and maintenance of a student record.
  iii. Administering access to services and facilities provided by or through the University as necessary to support your education 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 Student ID card, access control to buildings and/or facilities. This will include face-to-face and on-line services and facilities.

iv. The organisation and delivery of teaching events both at the University and in any other institution with which the University engages for providing part of your education.
v. Communicating with individual students and the student body, i.e. the dissemination of information to you from the University or any of its agents on (a) any matter(s) (internal or external) that are connected to your education and/or the services and facilities available to you as a student e.g. advising you of careers events, careers workshops and internship opportunities, of Sports Facilities and events provided by the Athletics Union etc. and (b) any matters necessary to maintain the health, safety and wellbeing of the University community.
    a. This will include the University making use of communication facilities and services provided by or through the University to students; and
    b. The University will transmit information to personal devices where a student has provided the University with the means to make contact through those devices, e.g. a mobile phone, external e-mail address, etc.
vi. The administration and execution of voluntary surveys of student opinion – connected with the assessment and development of the student experience and performance of the University.
vii. The organisation and administration of activities to assess your educational achievement and progress, e.g. written examinations, on-line tests, viva-voce.
viii. The determination whether academic work submitted is consistent with University requirements. This may include the application of measures to detect and prevent academic dishonesty, i.e. plagiarism detection services.
ix. Making decisions on academic progression, which may involve the exchange of information between Schools, Student Services and the Principal's Office.
x. The administration and execution of all processes/procedures concerning:
    a. Student complaints;
    b. Appeals (academic and non-academic); and
    c. Student discipline, which may involve the exchange of information between Schools, Student Services and the Principal's Office.
xi. The administration and the conferment of academic awards, i.e. graduation.

- <u>The provision of student support services</u>
    i. The administration and management of student residential services – including the monitoring and use of facilities for billing purposes.
    ii. The administration and provision of welfare and pastoral services. This could include professional counselling services provided by or through the University.
    iii. Careers guidance.
    iv. The admission and provision of financial support (grants, loans and bursaries etc.).
    v. The admission and provision of health care services provided by or through the University.
    vi. Liaison with third-parties to secure the safety, security and well-being of students.

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 to (under law), such as funding bodies and HESA[1] [2])
    a. NB the University when generating statistics will make every effort to remove any features that would allow a third-party to identify individuals from that information. Where personal data is made anonymous i.e. no identification of a living individual can be achieved from that data, then that information falls out of the scope of the DPA.
ii. Equal opportunities monitoring by the University or by external agencies which the University has an obligation to assist, such as funding bodies.
iii. Retention of evidence of student application, registration/enrolment, attendance, participation and performance as required by bodies such as the United Kingdom Visa and Immigration (UKVI), and the dissemination of such information to such agencies as prescribed by law so that they can undertake their prescribed functions.
iv. To exercise any other functions of a public nature, exercised in the public interest by any person – this may include the University taking steps to meeting a common law duty of care.

- Public safety and the prevention and detection of crime
    i. Images captured by Close 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, and in investigations where it is believed that University policy and/or regulation may have been breached.
    ii. Data from the University access control systems and/or logs of network and ICT facilities usage may be used to understand or determine whether a person 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 has been breached or for the prevention and detection of crime, or to identify the presence of a person where there are legitimate concerns over their personal safety and wellbeing.

- The maintenance of the University archive
    i. Core elements of the student 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

[1] The University is required by law, to make available to the relevant funding council(s), personal data on students. Those data are made available to the Higher Education Statistics Agency (HESA) either directly by the University or indirectly via a funding body. Details of the relevant legislation are available from: https://www.hesa.ac.uk/about/regulation/data-protection/guidance Accessed 21 July 2017.
[2] Details as to how HESA will make use of student personal data are available from privacy notices, published by that body. These are available from: https://www.hesa.ac.uk/about/regulation/data-protection/notices Accessed 21 July 2017.

provision of academic references, or developing an understanding of the composition of the student body over time.

- Alumni relations and fundraising
    i. Following graduation the University may use your personal data to make initial contact with you to keep you informed about the University, to offer you a range of alumni services, to advise you of potential opportunities to further your learning/studies and to support fundraising activities. Should you subsequently wish not to participate in those activities and signal that intent to the University, it will then cease to use your personal data in that way.

Transfer of personal data within the University

The University will from time to time pass personal data between Schools, Service Units and the Principal's Office as necessary to manage activities concerned with the:

- Provision of higher education and training;
- Management of the University – including the University meeting any legal and/or regulatory obligations; and
- Provision of student support services.

Transfer of personal data to third-parties

- Local authorities

  The Electoral Registration Officer (of a local authority) has powers through the Representation of the People Act(s) and the Representation of the People (Scotland) Regulations 2001 to secure information (including personal data) for the purposes of maintaining registers of parliamentary and local government electors. The University will pass student personal data to a local authority to support these purposes. The transfer of information in this circumstance does not require consent.

- Partner educational establishments

  The University will transfer personal data of students to partner institutions and other organisations e.g. work placement providers as necessary to manage and administer the provision of a higher education or training, the provision of student support services, the management of the respective partner institutions including meeting any legal and/or regulatory obligations, the maintenance of a (university) archive and alumni relations and fundraising.

- Relatives, guardians or carers of students

  Under normal circumstances the University will not disclose any personal data of students to any of their relatives, guardians, or carers etc. without the consent of a student. The University may, however, contact a student to inform them that another party wishes to make contact.

  Where a student has left the University for whatever reason, or they are not in attendance (e.g. a leave of absence) and a third-party makes enquiries about them, or seeks to contact them, assuming that they can be reached at the University, 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. By 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 student or another person are threatened

  The University may disclose the personal data and sensitive personal data of a student to others within the University and 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 student or another person. Vital interests in this context take the meaning as per that provided within the 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 student'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 student's life is permissible under law. This may include the passing of information made available to the University under confidence by a student, such as during a period of counselling. The University can also share sensitive (including that disclosed in confidence to it), without the consent of a student where it is not reasonable for it to obtain consent. Again, any transfer of information could only be made for the purposes of protecting vital interests (see above)

  The University will also normally confirm with the police and/or other authorities the details of a student's next of kin. The University may also take steps to notify next of kin where a student's vital interests (i.e. their physical and/or wellbeing) are or are believed to be threatened.

  The University may also make available to health care professionals details of a student'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 student.

  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 student 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.

Where the behaviour of a student raises significant cause for concern to the extent that the University has good reason to believe that the vital interests of a student or others are threatened, the University may then liaise with third-parties which could include relatives, guardians or carers of students without the consent and/or prior knowledge of the student to understand steps (if any) may be required to protect the vital interests of a student or others.

- Emergency contact(s)

  If an emergency arises, notably if a student is taken to hospital and they are unresponsive and/or it is not possible for the University to consult with that person to understand their wishes, the University may make contact with the person(s) that a student has informed the University are their emergency contact(s), without making any further reference to them (the student). Any personal data passed to an emergency contact will be the minimal amount of information required to advice that person(s) as to what the University understands to have happened to the student, so that the contact can begin to act in the student's interests.

- 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 s.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 named University Officers.

- The University of St Andrews Students' Association ("the SA")

  The University will pass onto the SA details of students so that the Association may then provide the relevant membership services to students, as per the relevant provisions of the Education Act 1994. If a student wishes to exercise their right not to be a member they can do so by contacting the SA offices.

- Publication of academic awards

  In addition to the publication of graduation lists, the University will maintain an online register of degree awards on its web site. This facility will allow potential employers to verify degree awards. The data published within this register will include a graduate's name, degree, classification and year of award. As the data within this register will be available world-wide via the Internet, occasions will arise where personal data is therefore transferred outwith the European Economic Area. Data from this register will only be made available in accordance with the instructions and permissions that are set by students and alumni.

Confirmation of student performance

The University routinely receives enquiries from potential employers seeking to validate claims made regarding educational performance, prior to offering employment to students or former students. The University will not release any personal data without having secured or confirmed the necessary consent from the individual concerned.

- References

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

- Publicity

  The University may from time to time take photographic and/or video images of University events and activities. Those present will be advised that that their images and their participation at an event etc. may be recorded. Images etc. may be used to promote an event and/or relevant University activities, in published literature and/or on-line. Normally where images etc. are to be captured, advance notice will be given or people will be advised at/during the event. Those present will then have the opportunity to either ask that they are not photographed etc. or alternatively there will be the option to leave or move elsewhere.

- Sponsors

  The University will pass a limited amount of information to sponsors for the purpose of managing invoices and the payment of fees. The University will not pass information to a sponsor concerning academic performance and/or progression unless this is a condition of sponsorship with which a student has consented or without first having secured consent of the individual concerned.

- 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 to 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.

Payment processing

The University will make available to third-party on-line payment processors e.g. WPM Education, minimal data (i.e. student ID number and date of birth) that will enable that party to validate on-line payments made by students for goods/services purchased from the University.

- Personal information secured by the University during student disciplinary investigations and proceedings

  Information secured by the University through the course of student 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.

How will the University use your sensitive personal data

The conditions legitimising the processing of sensitive personal data of students

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. In many instances it will be necessary for the University to secure the explicit consent of students 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 students at the point of data collection. In general terms the University may use sensitive personal data without first seeking the consent of students for the following purposes.

- To protect vital interests of students and others

  I.e. a life and death situation and/or where there is substantial risk to a person's property.

- To support legal proceedings, including preparing for proceedings

- Fraud prevention

- Health purposes i.e. disclosures to a health professional

- Equal opportunities monitoring and review

  Information on racial or ethnic origin may be used by the University to review data on the equality of opportunity and treatment of persons.

- The provision of confidential counselling services

  This could include making use of personal and sensitive personal data of a person who has been accused of abuse of someone undergoing counselling.

- Research – which is of substantial public interest

- Disability and data protection

  If a student 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 a higher education or training;
  - The provision of student services; or
  - The management of the University – including the University meeting any legal and/or regulatory obligations.

Mitigating circumstances

On occasion it may become necessary for students to seek to make representations to the University as to mitigating circumstances that they would like to be taken into consideration when decisions are being made on academic progression. For example a family bereavement, medical problem, financial difficulties etc. Where a student requests that mitigating circumstances to be taken into account, this is likely to involve the transfer of sensitive personal data between School(s), Student Services, Finance and the Principal's Office etc. This could involve the transfer of information

provided in confidence to personal tutors and Student Services etc. Where sensitive personal data is involved it will (in most instances) be necessary for the University to ask students to consent to the transfer of such information. If consent is not provided, this may then restrict the amount of information that will be available to those involved in the decision making process, which in turn may mean that not all circumstances can be taken into consideration.

The data protection principles

The following sections provide a brief overview as to how student 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 students 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 students will have sight of this Code prior to Registration and again during Registration.

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 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 then 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*." Students should ensure that all personal data they provide to the University is accurate, complete and up-to-date. Students 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.

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 students need to do if they wish to exercise these rights. In addition students also have the rights under the DPA.

6. 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. The University will also undertake processes of privacy by design and privacy impact assessments, to help ensure that privacy considerations are identified and feature as part of the design and delivery of systems and services that make use of personal data.

7. 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.

Availability

This Code will be published on the University website, and copies will be made to students each year at matriculation.

Contacts, further information

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