UNIVERSITY of STIRLING

DATA PROTECTION POLICY & GUIDANCE

Contents

Introduction

1 As the University processes 'personal data' of staff, students and other individuals, it is defined as a data controller for the purposes of the Data Protection Act 1998 (DPA). The University processes personal data strictly in accordance with the Act and its notification to the UK Information Commissioner's Office.

2 The University of Stirling is committed to a policy of protecting the rights and freedoms of individuals with respect to the processing of their personal data. This policy and guidance sets out the responsibilities of the University, its staff and its students to comply fully with the provisions of the Data Protection Act.

3 The Data Protection act applies to all data relating to, and descriptive of, living individuals defined in the Act as 'personal data'.

Data Protection Principles

4 The University is required to adhere to the eight principles of data protection as laid down in the DPA which means that information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. The eight principles are:

- Personal data shall be processed fairly and lawfully

- Personal data shall be held only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or purposes.
- Personal data shall be adequate, relevant and not excessive in relation to the purpose for which it is processed.
- Personal data shall be accurate and where necessary kept up to date.
- Personal data processed for any purpose shall not be kept for longer than is necessary for that purpose.
- Personal data shall be processed in accordance with the rights of data subject under the DPA.
- Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of the data.
- Personal data shall not be transferred to a country or a territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subject in relation to the processing of personal data.

5 University staff or others who process or use any personal information must ensure they follow these principles at all times.

6 The definition of 'processing data' includes obtaining/collecting, recording, holding, storing, organising, adapting, aligning, copying, transferring, combining, blocking, erasing and destroying the information or data. It also includes carrying out any operation or set of operations on the information or data, including retrieval, consultation, use and disclosure.

7 The University as data controller remains responsible for the control of personal data it collects even if that data is later passed onto another organisation or is stored on systems or devices owned by other organisations or individuals (including devices personally owned by members of staff).

Personal Data/Sensitive Personal Data

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

9 Examples which would **not** normally be classed as personal data include: attendance at meetings or mention in minutes, unless the meeting is about the named individual; University email address and telephone number, or names on emails/letters/memos unless the body of the document is about the named individual.

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

11 The DPA separately defines 'sensitive personal data' which relates to the following:

- The racial or ethnic origin of the data subject
- Their political opinions
- Their religious beliefs or other beliefs of a similar nature
- Whether they are a member of a trade union
- Their physical or mental health or condition
- Their sexual life
- The commission or alleged commission by them of any offence
- Any proceedings for an offence committed or alleged to have been committed by them, the disposal of such proceedings or the sentence of any court in such proceedings.

12 'Sensitive personal data' can only be processed under limited conditions which apply in addition to the general conditions for processing personal data set out in the DPA. These extra, more stringent, conditions are detailed in Schedule 3 of the DPA.

13 Where staff or students have disclosed a disability or other sensitive personal data, this information will be shared on a strictly need to know basis.

14 The University is required to obtain information about past criminal convictions as a condition of employment for certain posts. Disclosure Scotland checks are undertaken in respect of staff (and some students) who work with young and/or vulnerable people.

15 Particular care must also be taken with 'protected personal data' which is defined as any information that links one or more identifiable living person with information about them whose release would put them at significant risk of harm or distress. An example of this would be linking a person's name or address with information that could cause them harm such as their bank account details, passport number, criminal convictions, national insurance number etc. Protected personal data also covers any source of information containing 1000 or more identifiable individuals such as a database with more than 1000 entries.

Consent

16 In many cases, the University can only process personal data with the consent of the individual. When a member of staff starts working for the University or when a student undertakes their initial 'account discovery process' they will be asked to sign/accept a data protection statement giving the University consent to process their data. Staff or students who have concerns about signing this consent should contact the Data Protection Unit (data.protection@stir.ac.uk) however people should be aware that refusal to sign such a form, or give consent online, could result in the offer being withdrawn.

17 If an individual has provided personal data about themselves for a particular reason, then that individual has effectively given consent to the processing of their personal data but only for that purpose.

18 Unless there is explicit objection it is reasonable to assume that staff or students taking part in official events at which photographs, video or audio recordings are routinely taken e.g. graduation ceremonies and lectures, are content to appear.

19 The University also has to process 'sensitive personal data' e.g. for equal opportunities monitoring. It is recognised that the processing of sensitive data may cause particular concern or distress to individuals therefore staff and students will be asked to give express consent to the University to do this.

20 The University recognises that under the Act an individual can request that the University does not process information about him/her if that processing causes substantial unwarranted damage or distress. The University is not always bound to comply with the request. Individuals should be aware that, in some cases, by exercising this right they may disadvantage themselves. If you have concerns about the processing of data please contact the Data Protection Unit (data.protection@stir.ac.uk)

Information Held by the University

21 The University will expect to process personal data on a range of people including:

- Staff
- Applicants for employment
- Honorary, Emeritus and visiting staff
- Applicants for places
- Enrolled students
- Members of the Court and Conference and other lay committee members
- External examiners
- Consultants
- Customers and suppliers
- External members e.g. library, sports centre
- Research subjects
- Alumni
- Honorary graduates
- Actual and potential benefactors
- Staff and students next of kin or pension beneficiaries
- Complainants

22 When staff or students apply to the University they will provide some personal data as part of the application process. Through the course of employment or study additional information may be added to this record. During the period of employment or study personal information may be passed on to other areas of the University such as Information Services (for use of IT or library), Occupational Health, Student Support Services, Finance etc.

23 The University will process all personal data strictly in accordance with the DPA for legitimate administrative and business purposes.

24 Examples of processing staff data include:

- Managing HR processes e.g. salary and other payments, promotion, professional development reviews
- Absence management including sickness absence and annual leave
- Managing referrals to the Occupational Health
- Handling grievance matters, disciplinary cases, complaints and appeals
- Including staff details on the website
- Liaising with HMRC and pensions providers
- Maintaining contact with past employees
- Including contact details in academic publications or prospectuses/course material

25 Examples of processing student data include:

- To administer all aspects of the student interaction with the University e.g. admission, enrolment, supervision, attendance, assessment and graduation
- Provide advice and support on academic, pastoral and any relevant funding matters
- Administer the financial aspects of studying e.g. payment of fees, rents and collection of debts owed
- Providing information to professional bodies e.g. the Law Society of Scotland, Scottish Social Services Council
- Management of University services such as computing, library, student accommodation, careers service
- Compile records and statistics for research purposes, management information and to monitor equal opportunities policies
- For alumni activities, including fundraising
- Managing behavioural or disciplinary issues and complaints

26 Other uses of data include:

- Monitoring compliance with the Equality Act 2010
- Preventing and detecting crime e.g. by use of CCTV, including body warn cameras
- Making external/statutory returns e.g. to the Higher Education Statistics Agency (HESA), see section on 'Third Parties and Data Transfer' for further examples
- Transfer to other educational establishments or employers for the purposes of external study, placements or studying with partner institutions
- Organising insurance
- Consulting with legal advisers
- Audit investigations
- Maintenance/testing of information systems
- External debt collection agencies
- External survey providers carrying out staff or students surveys such as National Student Survey (NSS)
- Employers or potential employers of current or former students/staff

27 See also the section on '*Third Parties and Data Transfer*' below for a list of third parties that data may be transferred to.

Staff & Student Responsibilities

28 In relation to their own personal data staff and students should ensure that the information they provide to the University in connection with their studies or employment is accurate and up-to-date. Any change to information such as a new address should be notified to the University promptly. The University should also be informed if there are known to be any errors in their records. In the case of staff they should advise the Human Resources & Organisation Development (HR&OD) Office (hradmin@stir.ac.uk) of any changes and students should contact the Student Services Hub (ask@stir.ac.uk).

29 Deans of Faculty and Service Directors are responsible for ensuring that members of their Faculty/Service area process information in accordance with these guidelines. All users of personal information within the University have a responsibility to ensure that they process data in accordance with the eight Principles and these Data Protection Guidelines.

30 It is legitimate for Deans of Faculty/Service Directors to retain some basic information about staff in their area. The Human Resources & Organisation Development (HR&OD) Office will provide guidance on what may or may not be retained. When staff leave, all such information should be shredded or disposed of in confidential waste and electronic records should be deleted. It is not legitimate for members of staff in any other capacity to hold personal information on other members of staff without the latter's express consent. Where staff have access to personal data, such as the staff or student systems, they should only access data as required for their role.

31 Holding duplicate information leads to inaccuracies and extra care must be taken to ensure that all copies of personal data are updated. The data protection principles require that all information held is accurate and kept up to date.

32 As part of the recruitment process a single copy of the selection details should be retained for 6 months. Other individual members of staff should not retain any personal data on applicants, whether successful or not, after the conclusion of the appointment process. All such material should be shredded, disposed of in confidential waste or returned to HR&OD Office for disposal. Electronic records should be deleted.

33 Many members of staff will process data about students on a regular basis, for instance when compiling registers or marking coursework and examinations. The information that staff will deal with on a day to day basis will be ordinary personal data such as name, address, coursework marks and grades, and notes relating to matters such as behaviour or discipline. Staff with access to 'sensitive' personal data will be strictly limited on a need to know basis.

34 Members of staff supervising student work must ensure that the students adhere to these guidelines when using personal information.

35 Students who are considering processing personal data as part of their studies must notify and seek approval from their Supervisor/Dean of Faculty before any processing takes place. The member of staff should make the student aware of the requirements of the DPA and the appropriate security arrangements of the data. It is the responsibility of students to ensure they are compliant with DPA and the data protection principles.

Research

36 Data collected for the purposes of research are covered by the Act. They will however by exempt from Subject Access Requests if only intended for publication in such a way that individuals cannot be identified and is not being used to support measures or decisions with respect to a specific individual. It is therefore important to 'anonymise' the data as far as possible. Staff collecting data for the purpose of research or consultancy should incorporate an appropriate form of consent on any data collection form.

37 For further more detailed guidance on data protection and research see the Data Protection and Research Guidance Note.

Retention of Data

38 Personal data must only be kept for the length of time necessary to perform the processing for which it was collected. However, even after termination of employment or student relationship with the University, the University may still require to retain personal data to satisfy its obligations to keep certain records for particular periods under applicable law and/or as a way of maintaining a complete historical record.

39 For guidance on the retention of data see the webpage on Records Retention Guidance.

Subject Access Requests

40 The DPA gives data subjects the right to access personal information held about them by the University. The University may charge a fee for providing the information. The standard fee for a 'subject access request' is £10, payable in advance. For further guidance on how to make a subject access request please see the webpage Requesting Information from the University. The University must respond to all formal subject access requests within 40 calendar days.

41 Data subjects have the right to have any information held on them corrected if it is found to be incorrect and they have the right to prevent certain types of processing such as automatic decision taking, direct marketing, processing likely to cause substantial damage or substantial stress.

42 The rights of access include data held in unstructured manual filing systems. However the University will not be obliged to disclose such data unless the data subject can provide a description of it, nor if the costs of locating it exceed the maximum search costs allowed under the Freedom of Information Act, currently £450.

43 References are discloseable to the person about whom they are written under the subject access provisions of the DPA. This includes references received by the University from external sources as part of an application process and confidential references given and received internally e.g. as part of advancement and promotions procedures. There is an exemption under the Act from disclosure for references written by University staff and sent externally, however this reference may still be accessible by the applicant from the organisation to which the reference was sent. For further

guidance on giving references please see the Issuing of Staff and Student References Advisory Note. In order to maintain confidentiality and to prevent the unauthorised disclosure of information, staff should not provide references without a prior request from the student concerned.

Examination Marks

44 The University is not required by law to disclose examinations scripts, however students are entitled to any marks or comments annotated on the script. Students are entitled to their marks for both coursework and examinations. Unpublished marks must be disclosed within 5 months of a Subject Access Request.

Third Parties and Data Transfer

45 The University will only disclose your data to external third parties where we:

- Have your consent; or
- Are required to under a statutory or legal obligation; or
- Are permitted to do so by the DPA

46 To fulfil our statutory or legal obligations your data may be provided, without your explicit consent, to these organisations or agents acting on their behalf (web links provide additional information):

- The Higher Education Statistics Agency (HESA)
- The Scottish Funding Council (SFC)
- The Student Loans Company (SLC)
- The Student Awards Agency for Scotland (SAAS)
- Home Office/UK Border Agency (UKBA)
- Higher Education Funding Council for England (HEFCE) including agents managing the Research Excellence Framework (REF)
- HM Revenue & Customs (HMRC)
- University of Stirling Students' Union
- Pension providers
- Embassies
- Other Government departments and agencies including local councils for council tax exemptions and Electoral Registration Officers for electoral registers.

47 The University may use some external agencies to process data on its behalf where it is necessary for the business of the University. Some examples of this are the use of Graduate Prospects Limited (to administer Career Development Centre Functions) and Hobsons Enrolment Management Services (to allow the University to monitor and report on enrolment statistics). In these cases there will be a written contract between the parties which specifies that the data processor agrees to act on the University's instructions and to abide by the provisions of the DPA in connection with data security.

48 The University may require to transfer personal data to external agencies (to allow those agencies to transfer personal data on its behalf) outside the European Economic Area (including subcontractors of Hobson Enrolment Management Services) to process personal data on its behalf where it is necessary for the business of the University, as

set out in paragraph 47 above. The DPA lists the factors that should be considered to ensure an adequate level of protection for the data and some exemptions under which the data can be exported. Information published on the internet must be considered to be an export of data outside the EEA. This covers data stored in the Cloud unless the service provider explicitly guarantees data storage only takes place within the EEA.

49 The Information Commissioner's Office Guidance on the use of Cloud Computing should be consulted before any use of external computing resources or services via a network which may involve personal data.

50 Relevant information may also be disclosed as permitted under the DPA to parties such as the Police. See separate staff guidelines on Requests for Personal Information from Third Parties which gives detail on how to deal with common requests from third parties such as requests from relatives, police, local councils etc.

Data Security

51 All University users of personal data must ensure that all personal data they hold is kept securely. They must ensure that it is not disclosed to any unauthorised third party in any form either accidentally or otherwise.

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

53 Staff and students must adhere to their data security obligations as defined in the prevailing version of the University's Information Technology Use Policy.

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

55 All personal data must be treated as confidential information and destroyed appropriately.

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

Direct Marketing

57 Direct marketing relates to communication (regardless of media) with respect to advertising or marketing material that is directed to individuals e.g. mail shots for fund raising, advertising short courses etc. Individuals must be given the opportunity to remove themselves from lists or databases used for direct marketing purposes.

58 Direct marketing must also comply with the Privacy and Electronic Communications (EC Directive) Regulations 2003.

Complaints/Disciplinary Action

59 Data may only be processed in accordance with this policy and with the terms of the University's notification to the Information Commissioner (Ref: Z5416027). The Information Commissioner's Office publishes details of all registered Data Controllers and this is available for inspection at their website (https://ico.org.uk). Any breach of the policy may result in the University, as the registered Data Controller, being liable in law for the consequences of the breach.

60 Any member of staff or student who is found to have made an unauthorised disclosure of personal information or breached the terms of this Policy may be subject to disciplinary action. Staff may also incur criminal liability if they knowingly or recklessly obtain and/or disclose personal information without the consent of the University i.e. for their own purposes, which are outside the legitimate purposes of the University.

Conclusion

61 Compliance with the Data Protection Act is the responsibility of all members of the University. Any deliberate breach of this Policy may lead to: disciplinary action being taken, access to University facilities being withdrawn, or even criminal prosecution.

62 Before processing personal data, all staff should consider the following:

- Do you really need to record the information?
- Is the information 'ordinary' personal data or is it 'sensitive' personal data?
- If it is sensitive personal data, do you have the data subject's explicit consent?
- Has the subject been told that this type of data will be processed?
- Are you authorised to collect/store/process the personal data?
- Have you checked with the data subject that the personal data is accurate?
- Are you sure that the personal data will be secure during the process?
- If you do not have the data subject's consent to process, are you satisfied that the collection/retention of personal data is permitted in terms of DPA?

Contact Details

63 For further information or advice about data projection issues please contact:

Data Protection Unit
Policy & Planning
University of Stirling
Stirling
FK9 4LA

Email: data.protection@stir.ac.uk
Tel: 01786 466940

Policy & Planning
October 2013. Updated May 2015, May 2016, August 2016