DATA PROTECTION POLICY V3.1

19/03/2018

Elaine Grant, Data Protection Officer

Version control and history

Title	Description	Author	Approval
University Data Protection Policy	1st version of the University's Data Protection Policy in relation to 1998 legislation.	Craig Williamson	University Court. October 2001
Data Protection Policy v2.0	Major redraft of the above policy.	Elaine Forbes	Information Strategy Committee 25 October 2012
Data Protection Policy v2.1	Minor amendments to update outdated links in section 10.	Elaine Grant	Updated 06 January 2017. Approval not required due to minor nature of amendments.
Data Protection Policy v2.2	Minor amendment to refer to University Secretary and Compliance Officer	Elaine Grant	Update 13 December 2017. Approval not required due to minor nature of amendments
Data Protection Policy v3.0	Major redraft to ensure compliance with General Data Protection Regulation	Elaine Grant	Digital Campus Sub-Committee 23 May 2018
Data Protection Policy v3.1	Point 4.3 included Name of v3.0 changed in this front table from 'Data Protection and Privacy Policy v3.0' to 'Data Protection Policy v3.0'	Elaine Grant	Update 19/03/2019 Approval not required due to minor nature of amendments

Contents

1. Introduction

1.1 The University of Strathclyde needs to collect, process and retain certain information about its employees, students (potential, current and former) and other individuals for various purposes, e.g.: managing the academic career and progress of student; recruiting, managing and paying staff; undertaking research; complying with legal or statutory obligations etc. 'Personal data' is information which relates to an identifiable living individual who can be directly or indirectly identified from the information. Personal data must be processed in accordance with data protection legislation.

1.2 Data protection legislation has existed in the UK for many years. On 25 May 2018 the General Data Protection Regulation (GDPR) comes into force, replacing the Data Protection Act 1998. UK legislation will also be passed to implement national derogations.[1]

1.3 The University has formally adopted this policy to ensure compliance with GDPR and related privacy legislation.

1.4 The University is the 'data controller', as defined by the legislation.

1.5 The policy will be available at all times via our website www.strath.ac.uk/dataprotection.

2. Purpose

2.1 The policy sets out the University's commitment to comply with data protection and associated privacy legislation. It sets out the responsibilities of the University, its staff, its students and others as defined in this policy in relation to data protection compliance.

2.2 This policy and associated policies, procedures and guidance form a framework within which those processing personal data should operate. This framework will assist the University in complying with its legal obligations.

3. Policy Statement

3.1 The University is committed to protecting the rights and freedoms of individuals in relation to the processing of their personal information.

3.2 The University will process personal data in accordance with the legislation and best practice.

4. Scope and status

4.1 This policy applies to all University staff, students and others who use or process any personal data for University purposes, irrespective of where the personal data is processed. The policy applies to all personal data or special category data held in electronic form or in (structured) manual paper records.

[1] As at 3 May 2018 the UK Data Protection Bill has not yet been passed.

4.2 In addition to information identified in 1.1 and 4.1, personal data also includes images (still and moving) and audio recordings (from which an individual can be identified). CCTV is covered by this policy although there is a separate CCTV Code of Practice.

4.3 For the avoidance of doubt, this policy is also intended to fulfil the requirement to have an appropriate policy document in place when relying on the substantial public interest conditions under Schedule 1, Part 2 of the Data Protection Act 2018.

5. Responsibilities of Staff

5.1 The University Secretary and Compliance Officer has overall institutional responsibility for compliance with this policy and the legislation.

5.2 Deans, Directors and Senior Officers (with responsibility for non-academic departments) are ultimately responsible for ensuring that their areas are compliant with this policy and that the annual Data Protection Audit (DP Audit) is completed.

5.3 Heads of School/Department (academic and service) have direct responsibility for ensuring that their area complies with the legislation and that the annual DP Audit is completed.

5.4 The Data Protection Officer (DPO) is responsible for the production and maintenance of this policy. The DPO assists the University in monitoring internal compliance, informing, advising and training staff on data protection obligations, and acts as a contact point for data subjects and the supervisory authority, the Information Commissioner's Office (ICO).

5.5 The Information Governance Unit (IGU), under the direction of the DPO, provides advice and guidance in relation to data protection matters throughout the University and is responsible for overseeing the handling of requests in relation to data subjects' rights.

5.6 A departmental Data Protection Contact should be appointed for every business area/dept. to: promote awareness; advise colleagues; disseminate information; assist the IGU in responding to requests from data subject. It is the responsibility of the Head of Department/Director to appoint a DP Contact. If no Contact is appointed the Head of Department/Director assumes the role. The IGU must be notified as to who the DP Contact is.

5.7 All staff, including those covered by ongoing and fixed term employment contracts, assignments or visiting and honorary appointments must comply with this Policy, the GDPR and the UK Data Protection Act (when it comes into force) whenever processing personal data held by the University or on behalf of the University. Staff must ensure that they understand the requirements of GDPR. Training, resources, advice and guidance is available via the IGU.

6. Responsibilities of Third Parties Working on Behalf of the University

6.1 The University is responsible for the processing of personal data by third party companies or individuals working on its behalf.

6.2 Where the University engages or appoints a third party to process personal data on its behalf e.g. consultants; contractors; agents; external examiners/supervisors; or trustees those individuals must be required to comply with data protection legislation. The staff responsible for the activity must ensure appropriate agreements are in place to safeguard personal data, e.g. data processing agreements.

7. Responsibilities of Students

7.1 All students processing personal data on behalf of the University (as data controller) are responsible for compliance with the rules and policies of the University.

7.2 Students who are considering processing personal data as part of their studies must gain approval from the appropriate member of academic staff before processing takes place.

7.3 Students are responsible for ensuring that information they supply is accurate and that they inform the University of any updates/changes or update this information themselves via University systems.

8. Data Protection Principles

The GDPR requires that personal data is processed in line with the 6 principles, namely that personal data shall be:

(a) processed lawfully, fairly and in a transparent manner ('lawfulness, fairness and transparency');
(b) collected for specified, explicit and legitimate purposes and not further processed in any manner incompatible with those purposes. Further processing for archiving, scientific or historical research or statistical purposes is permissible ('purpose limitation');
(c) adequate, relevant and limited to what is necessary in relation to the purpose for which it is processed ('data minimisation');
(d) accurate and where necessary kept up to date ('accuracy');
(e) not be kept for longer than is necessary for that purpose ('storage limitation');
(f) processed in a manner that ensures appropriate security including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

In addition, the accountability principle as set out in Article 5(2) requires that:

"the controller shall be responsible for, and be able to demonstrate, compliance with the principles."

9. Records of Processing Activities

9.1 The University is required to maintain a record of processing activities which records information relating to the processing of personal data, including: the purpose of processing; the types of individuals about who data is held; who personal information is shared with; when data is transferred to countries outside the EU.

9.2 All departments must complete an annual DP Audit, the content of which is determined by the DPO/IGU. The University currently records processing activities from the information supplied in these audits.

9.3 Departments will be required to complete and maintain any other such register developed by the University to record processing activities.

10. Privacy Notices

10.1 In order to comply with the requirements in relation to 'fairness and transparency', under the first principle, the University shall ensure that it provides adequate information to data subjects as to how their personal data will be used.

10.2 The central staff and student privacy notices can be found at [under development – insert link when appropriate].

10.3 Any processing outwith the scope of the central staff/student privacy notices, or where special category data is involved, may require a separate privacy notice to be provided. Additional privacy notices may be self-contained or may refer back to a central notice to provide 'layered' privacy information, as appropriate.

11. Information Security

11.1 Whenever personal data is being processed appropriate technical and organisational measures must be taken to ensure the security of that data.

11.2 Those processing personal data must act in accordance with relevant University IT/Cyber Security policies and procedures.

11.3 Departmental measures to ensure security will also be required, e.g. in relation to secure storage, access limitation, secure transfer methods and not disclosing information inappropriately e.g. in writing or orally.

11.4 Further information and advice in relation to methods of secure IT storage/ transfer can be obtained from the University's IT & Technical Services department.

12. Personal Data Breach

12.1 All necessary measures should be taken to avoid data breaches occurring. Examples of personal data breaches include:

- personal information sent in an email to the wrong recipient;
- personal information loaded on to a website by mistake;
- unencrypted storage/memory, device or laptop lost or left unattended;
- files containing personal data left in a public place;
- hackers gaining access to confidential files;
- unauthorised staff able to access files containing personal data;
- theft of a laptop or bag containing files;

- personal data left in an unsecured location i.e. a shared drive accessible to all staff or an unlocked filing cabinet in an open-access area.

12.2 If a data breach does occur staff must follow breach reporting procedures to ensure the University is able to comply with its legal obligations to report any breach which is likely to result in a risk to the rights and freedoms of Data Subjects to the Information Commissioner's Office within 72 hours of becoming aware of the breach.

12.3 Breach reporting procedures are available via ISD/IGU Sharepoint sites and will be reviewed and updated as required.

13. Individuals' Rights

13.1 GDPR gives individuals a number of specific rights, depending on the circumstances, namely:

- the right to be informed;
- the right of access;
- the right to rectification;
- the right to erasure;
- the right to restrict processing;
- the right to data portability;
- the right to object;
- rights in relation to automated decision making and profiling.

13.2 The University will develop procedures and guidance to ensure that staff across the University are able to comply with these rights, as required.

14. Retention and Disposal of Personal Data

14.1 Personal data shall only be required as long as necessary for the purpose for which it was collected.

14.2 The University will develop, maintain and implement retention policies to retain personal data for the length of time required for the specified purpose.

14.3 Retention schedules will be based on legal, business and best practice requirements and will be publicised to ensure transparency.

14.4 Some personal data may be retained permanently in the University Archives.

15. Privacy by Design

15.1 The University will consider the impact on data privacy during all processing activities. This includes implementing measures to ensure that privacy and the protection of data is considered during the design stage of a process and to use

appropriate technical and organisational measures to minimize the risk to personal data.

15.2 Procedures will be developed and implemented to ensure that Data Protection Impact Assessments (DPIAs) are undertaken where necessary. DPIAs are a mechanism for identifying and examining the impact of new initiatives and putting in place measures to minimize or reduce privacy risks.

16. Direct Marketing

16.1 Direct marketing, when it involves the use of personal data, must be conducted in accordance with this policy.

16.2 Unsolicited direct marketing by electronic means also requires the University to comply with the requirements of the Privacy and Electronic Communications (EC Directive) Regulations 2003 [PECR] and any subsequent legislation which replaces these Regulations.

17. Research

17.1 The University's research policies and procedures and ethical approval processes will address GDPR requirements in relation to research.

18. Impact of Non-compliance

18.1 Any individual who is found to have breached the policy and/or who is found to have made an unauthorised disclosure of personal information may be subject to disciplinary action.

18.2 Staff may also incur criminal liability if they knowingly or recklessly obtain and/or disclose personal information without the consent of the University.

18.3 The University may face investigation and enforcement action by the ICO in case of non-compliance. This can include substantial fines. The level of fine depends on the scale and nature of the breach and the privacy impact to individuals.

19. Review

19.1 This policy will be subject to review every three years, or as required, in order to comply with any changes in UK/EU guidance or legislation.

19.2 Minor amendments, e.g. typographical errors or updates to legislative references will be made by the DPO without formal approval.

19.3 Any significant amendments will require the policy to be submitted for approval via the appropriate process.