University of Cambridge

Data Protection Policy

1 Purpose and scope

1.1 The purpose of this policy is to ensure compliance with the UK General Data Protection Regulation, the Data Protection Act 2018 and related legislation ('data protection law').[1] Data protection law applies to the storing or handling ('processing') of information ('personal data') about living identifiable individuals ('data subjects').

1.2 This policy applies to all parts of the University of Cambridge ('the University'), as a single organisation ('data controller'), with the exception of Cambridge University Press & Assessment.[2] It does not apply to the Colleges, associated Trusts or subsidiary companies, which are separate legal entities and data controllers.

1.3 This policy applies to all staff except when acting in a private or non-University capacity. In this policy, the term 'staff' means anyone working in any context within the University at whatever level or grade and whether permanent, fixed term or temporary, including but not limited to employees, retired but active research staff, other visiting research or teaching staff, workers, trainees, interns, seconded staff, agency staff, agents, volunteers, and external members of committees.

1.4 This policy applies to all students when processing personal data on behalf of the University, but not in any other situation including when acting in a private or non-University capacity.

1.5 This policy is not, and should not be confused with, a privacy notice (a statement informing data subjects how their personal data is used by the University).[3]

1.6 This policy should be read in conjunction with the obligations in the following documents, which supplement this policy where applicable:

1.6.1 staff employment contracts and comparable documents (e.g. worker agreements), which impose confidentiality obligations in respect of information held by the University;[4]

1.6.2 information security policies, procedures and terms and conditions, which concern the confidentiality, integrity and availability of University information, and which include rules about acceptable use, breach reporting, IT monitoring, and the use of personal mobile devices;[5]

---

[1] Links to full legislative texts are published at https://www.information-compliance.admin.cam.ac.uk/data-protection#heading1.

[2] Cambridge University Press & Assessment has its own data protection policies.

[3] For which see https://www.information-compliance.admin.cam.ac.uk/data-protection#heading3.

[4] See https://www.recruitment.admin.cam.ac.uk/resources-and-support/contractual-terms.

[5] See https://help.uis.cam.ac.uk/service/security/rules and related webpages.

1.6.3 records management policies and guidance, which govern the appropriate retention and destruction of University information;[6] and

1.6.4 any other contractual obligations on the University or individual staff or students which impose confidentiality or data management obligations in respect of information held by the University, which may at times exceed the obligations of this and/or other policies in specific ways (e.g. in relation to storage or security requirements for funded research).

2 Policy statement

2.1 The University is committed to complying with data protection law as part of everyday working practices.

2.2 Complying with data protection law may be summarised as but is not limited to:

2.2.1 understanding, and applying as necessary, the data protection principles when processing personal data;[7]

2.2.2 understanding, and fulfilling as necessary, the rights given to data subjects under data protection law;[8] and

2.2.3 understanding, and implementing as necessary, the University's accountability obligations under data protection law.[9]

3 Roles and responsibilities

3.1 The University has a corporate responsibility as a data controller (or when acting as a joint data controller or a data processor) for:

3.1.1 complying with data protection law and holding records demonstrating this;

3.1.2 cooperating with the Information Commissioner's Office (ICO) as the UK regulator of data protection law; and

---

[6] See https://www.information-compliance.admin.cam.ac.uk/records-management.

[7] The principles in relation to personal data are: lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation; and integrity and confidentiality.

[8] The data subject rights are: to be informed; access; rectification; erasure; restriction; data portability; and objection (including in relation to automated decision-making).

[9] The accountability obligations include: implementing appropriate data protection policies; implementing data protection by design and default in projects, procurement and systems; using appropriate contracts with third party data controllers and data processors; holding relevant records about personal data processing; implementing appropriate technical and organisational security measures to protect personal data; reporting certain personal data breaches to the Information Commissioner's Office; conducting Data Protection Impact Assessments where required; and ensuring adequate levels of protection when transferring personal data outside the UK.

3.1.3 responding to regulatory/court action and paying administrative levies and fines issued by the ICO.

3.2 The University Council is responsible for:

3.2.1 reviewing (at least once every five years) and approving this policy; and

3.2.2 assessing the overall risk profile and ensuring appropriate resources and processes are in place and implemented to enable compliance with data protection law.

3.3 The independent University Data Protection Officer is responsible for:

3.3.1 monitoring and auditing the University's compliance with data protection law, especially its overall risk profile, and reporting annually to the University Council;

3.3.2 advising the University, usually through its Information Compliance Office,[10] on all aspects of its compliance with data protection law (including its use of Data Protection Impact Assessments);

3.3.3 acting as an available point of contact with the ICO with regard to data protection law; and

3.3.4 acting as an available point of contact for complaints from data subjects.

3.4 The Information Compliance Office, in collaboration with other relevant offices, is responsible for:

3.4.1 providing advice, guidance, training and tools/methods, in accordance with the University's overall risk profile and having taken into account the advice of the independent Data Protection Officer, relevant case law and ICO/other regulatory guidance, to help University Institutions and staff comply with this policy;

3.4.2 publishing and maintaining core privacy notices and other University-wide data protection documents (including this policy);

3.4.3 handling data subject rights requests; and

3.4.4 in collaboration with the University Data Protection Officer, managing and/or handling Data Protection Impact Assessments, data subject complaints and personal data breaches, including liaising with the ICO on these and any other matters as necessary.

3.5 Heads of Institutions are responsible for:

[10] Within the Governance and Compliance Division (a Division of the Unified Administrative Service).

3.5.1 making all staff within their Institution aware of this policy as necessary;

3.5.2 ensuring that appropriate processes, training and assurance activities are implemented and/or carried out within their Institution to enable compliance with data protection law;[11] and

3.5.3 ensuring that appropriate processes are implemented within their Institution to enable information assets containing personal data within their Institution to be included in the University's Information Asset Register.

3.6 Individual staff, as appropriate for their role and in order to enable the University to comply with data protection law, are responsible for:

3.6.1 completing relevant data protection training;[12]

3.6.2 following relevant advice, guidance and tools/methods provided by the Information Compliance Office (and other relevant offices) depending on their role, regardless of whether access to and processing of personal data is through University-owned and managed systems, or through their own or a third party's systems and devices;

3.6.3 when processing personal data on behalf of the University, only accessing and using it as necessary for their contractual duties and/or other University roles and not disclosing it unnecessarily or inappropriately;

3.6.4 recognising, reporting internally, and cooperating with any remedial work arising from personal data breaches;

3.6.5 recognising, reporting internally, and cooperating with the fulfilment of data subject rights requests;

3.6.6 when engaging with students who are using personal data in their studies and research, advising those students of relevant advice, guidance and tools/methods to enable them to handle such personal data in accordance with this policy; and

3.6.7 only deleting, copying or removing personal data when leaving the University as agreed with their Head of Institution (or an appropriate delegate) and as necessary.

3.7 The responsibilities in paragraph 3.6 apply to individual students when processing personal data on behalf of the University.

---

[11] With regard to training, all staff using personal data in some way in their role are expected, as a foundation, to complete the main online data protection course (see https://www.training.cam.ac.uk/cppd/course/cppd-dataprot) as part of their induction and thereafter once every two years. Supplementary expectations about data protection training in different areas of the University are set by Heads of Institutions (and equivalents).

[12] See footnote 11.

3.8 Non-observance of the responsibilities in paragraph 3.6 may result in disciplinary action.

3.9 The roles and responsibilities in paragraphs 3.1 to 3.8 do not waive any personal liability for individual criminal offences for the wilful misuse of personal data under data protection law.[13]

4 Contact and date of last revision

4.1 Contact details are published on the Information Compliance Office's webpages.[14]

4.2 This policy was last reviewed and approved by the University Council in March 2023.[15]

[13] These criminal offences include: unlawfully obtaining, disclosing or retaining personal data; recklessly re-identifying de-identified personal data without the data controller's consent; deliberately altering or deleting personal data to prevent disclosure in accordance with data subject access rights; forcing a data subject to exercise their access rights; and knowingly giving false statements to the ICO.

[14] See https://www.information-compliance.admin.cam.ac.uk/contact-us.

[15] Prior to this date the first version of the policy was in force from March 2018 to March 2023. Footnotes 11 and 12 were added in July 2024 as editorial corrections.