Version number: 1.0
Regulation owner: Data Protection Officer
Effective date: 24/04/2018
Review date: 24/04/2021

University of Chichester

PRIVACY STANDARD

Approved by the Board of Governors: 24 April 2018

University of Chichester
PRIVACY STANDARD

TABLE OF CONTENTS

1. KEY TERMS

Applicable data protection legislation The UK Data Protection Act 1998, the EU General Data Protection Regulation ((EU) 2016/679) and any applicable equivalent or replacement legislation.	**Consent** Agreement which is freely given, specific, informed and unambiguous.	**Data Breach** A personal data breach means the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This means that a breach is more than just losing personal data.
Data Controller The person or organisation that determines when, why and how to Process Personal Data.	**Data Privacy Impact Assessment** Also: **DPIA**. A standard assessment used to identify and reduce risks of a data processing activity.	**Data Processor** Any person, company or organisation (other than an employee of the data controller) who processes Personal Data on behalf of a Data Controller.
Data Protection Officer (DPO) An internal, statutory role, required to monitor and promote compliance with data protection legislation.	**Data Subject** Any living, identified or identifiable individual about whom we hold Personal Data.	**Data Subject Rights** The rights granted to Data Subjects by the applicable data protection legislation, including the right of access to their Personal Data, the right to correct it, and the right to deletion (see below, section 12).
Personal Data Any information identifying a Data Subject or from which we could identify a Data Subject. Personal Data includes "Special Categories" of sensitive personal data and Pseudonymised Data but not anonymised data (data where any identifying elements have been removed).	**Special Categories of Personal Data** A special subset of Personal Data, being any information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life or sexual orientation, biometric or genetic data, and Personal Data relating to criminal offences and convictions.	**Processing** or **Process** Any activity that involves the use of Personal Data, whether manual or electronic, including obtaining, recording or holding the data, organising, amending, transferring, retrieving, using, disclosing, erasing or destroying it.
Privacy Notices Separate notices setting out information that may be provided to Data Subjects when the University collects information about them. These notices may apply to a specific group of individuals (for example, employees) or they may cover a specific purpose (such as filming on campus).	**Pseudonymised Data** Data which has been modified to replace information that directly or indirectly identifies an individual with artificial identifiers or pseudonyms so that the person, to whom the data relates, cannot be identified without the use of additional information which is kept separately and secure.	**Third Party** Anyone other than the Data Subject and the Data Controller.

2. INTRODUCTION

2.1 Protecting the confidentiality and integrity of Personal Data is a critical responsibility that the University of Chichester (the **University**) takes seriously at all times. We recognise that the correct and lawful treatment of Personal Data will maintain confidence in the University and its operations.

2.2 This Privacy Standard sets out how the University manages the Personal Data of our students, employees, workers, suppliers and other third parties.

2.3 This Privacy Standard applies to all Personal Data we Process regardless of how that data is stored or whether the Data Subject has an ongoing, past or future relationship with us.

2.4 This Privacy Standard applies to all University employees, students and all third-party contractors working on the University's behalf. You must read, understand and comply with this Privacy Standard when Processing Personal Data on behalf of the University and attend training as appropriate to your role. This Privacy Standard sets out what we expect from you in order for the University to comply with applicable law. Your compliance with this Privacy Standard is mandatory. Any breach of this Privacy Standard may result in disciplinary action.

2.5 Breach of the applicable data protection legislation could result in potential fines of up to EUR20 million (approximately £18 million) or 4% of our total worldwide annual turnover, whichever is higher.

3. MANAGEMENT

3.1 All staff with management responsibilities are responsible for ensuring compliance with this Privacy Standard and must implement appropriate practices, processes, controls and training to ensure such compliance.

3.2 The DPO is responsible for overseeing this Privacy Standard and, as applicable, developing additional guidance and procedures. The University's DPO is Su Longden, who is contactable on DPOfficer@chi.ac.uk or on 01243 81 6020.

3.3 Please contact the DPO with any questions about the operation of this Privacy Standard or the applicable data protection legislation or if you have any concerns that this Privacy Standard is not being or has not been followed. In particular, you must always contact the DPO in the following circumstances:

3.3.1 if there has been a Data Breach;

3.3.2 if you are intending to transfer Personal Data outside the EEA;

3.3.3 if a Data Subject invokes their rights, for example, to a copy of all data we hold on them, or their right to be forgotten (see below);

3.3.4 whenever you are engaging in a significant new, or change in, Processing activity which is likely to require a DPIA (see below);

3.3.5 if you plan to use Personal Data for purposes others than what it was collected for; or

3.3.6 If you plan to undertake any activities involving Automated Processing or Automated Decision-Making (see below).

4. PERSONAL DATA PROTECTION PRINCIPLES

4.1 Under the applicable data protection legislation, Personal Data must:

4.1.1 be Processed lawfully, fairly and in a transparent manner (**Lawfulness, Fairness and Transparency**);

4.1.2 be collected only for specified, explicit and legitimate purposes (**Purpose Limitation**).

4.1.3 be adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed (**Data Minimisation**).

4.1.4 be accurate and where necessary kept up to date (**Accuracy**).

4.1.5 not be kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the data is Processed (**Storage Limitation**).

4.1.6 be Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful Processing and against accidental loss, destruction or damage (**Security, Integrity and Confidentiality**).

4.1.7 not be transferred to another country without appropriate safeguards being in place (**Transfer Limitation**).

4.1.8 be made available to Data Subjects and Data Subjects allowed to exercise certain rights in relation to their Personal Data (**Data Subject's Rights and Requests**).

4.2 We are responsible for and must be able to demonstrate compliance with the data protection principles listed above (**Accountability**).

5. PERSONAL DATA ABOUT CHILDREN

5.1 The University regards anyone under the age of 16 as a child for the purposes of data protection.

5.2 Children have the same rights as adults over their personal data and can exercise their own rights as long as they are competent to do so. Where a child is not considered to be competent, an adult with parental responsibility may exercise the child's data protection rights on their behalf. When we offer an online service directly to a child, the applicable data protection legislation states that only children aged 13 or over are able provide their own consent.

5.3 This Privacy Standard applies equally to children as it does to adults. In addition, when dealing with Personal Data belonging to a child:

5.3.1 when relying on consent, we will make sure that the child understands what they are consenting to, and we do not exploit any imbalance in power in the relationship between us;

5.3.2 when relying on 'necessary for the performance of a contract', we will consider the child's competence to understand what they are agreeing to, and to enter into a contract;

5.3.3 when relying upon 'legitimate interests', we will take responsibility for identifying the risks and consequences of the processing, and put age appropriate safeguards in place.

5.4 Guidance and Privacy Notices directed towards children should be written in a concise, clear and plain style and age-appropriate.

5.5 The right to erasure is particularly relevant when an individual originally gave their consent to processing when they were a child.

6. LAWFULNESS, FAIRNESS, TRANSPARENCY

Lawfulness and Fairness

6.1 Personal data must be Processed lawfully, fairly and in a transparent manner in relation to the Data Subject.

6.2 We may only collect, Process and share Personal Data fairly and lawfully and for specified purposes. The applicable data protection legislation restricts our actions regarding Personal Data to specified

lawful purposes. These restrictions are not intended to prevent Processing, but ensure that we Process Personal Data fairly and without adversely affecting the Data Subject.

6.3 The applicable data protection legislation allows Processing for specific purposes, some of which are set out below:

6.3.1 where the Data Subject has given his or her Consent;

6.3.2 where the Processing is necessary for the performance of a contract with the Data Subject;

6.3.3 to meet our legal compliance obligations;

6.3.4 to protect the Data Subject's vital interests;

6.3.5 to pursue our legitimate interests (where the Processing does not prejudice the interests or fundamental rights and freedoms of Data Subjects); or

6.3.6 where the Processing is necessary in the performance of a public task.

6.4 You must identify and document the legal ground being relied on for each Processing activity.

Consent

6.5 Where we rely on the Consent of the Data Subject as our lawful basis for Processing, Consent must be indicated clearly either by a statement or positive action in respect of the Processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity are unlikely to be sufficient. If Consent is given in a document which deals with other matters, then the Consent must be kept separate from those other matters.

6.6 Data Subjects must be easily able to withdraw Consent to Processing at any time and withdrawal must be promptly honoured. Consent may need to be refreshed if you intend to Process Personal Data for a new purpose which was not disclosed when the Data Subject first consented.

6.7 Where we rely on Consent for Processing Special Categories of Personal Data, for automated decision-making processes or for cross border data transfers, that consent must be explicitly given. Usually we will be relying on another legal basis (and so will not require explicit consent) to Process most types of Special Categories of Personal Data. Where explicit consent is required, you must issue a Privacy Notice to the Data Subject to capture explicit consent.

6.8 You will need to evidence Consent captured and keep records of all Consents so that the University can demonstrate compliance with Consent requirements.

Transparency (Notifying Data Subjects)

6.9 The applicable data protection legislation requires Data Controllers to provide detailed, specific information to Data Subjects as to what information is being collected about them. Such information must be provided through appropriate Privacy Notices which must be concise, transparent, intelligible, easily accessible, and in clear and plain language so that a Data Subject can easily understand them.

6.10 Whenever we collect Personal Data directly from Data Subjects we must provide the Data Subject with a Privacy Notice that states the identity of the Data Controller and DPO and how and why we will use, Process, disclose, protect and retain that Personal Data. The Privacy Notice must be supplied before the data is collected.

6.11 When Personal Data is collected indirectly (for example, from a third party or publically available source), you must provide the Data Subject with the same information as soon as possible after collecting/receiving the data. You must also check that the Personal Data was collected by the third party in accordance with the applicable data protection legislation and on a basis which allows for our proposed Processing of that Personal Data.

6.12 The University has certain standard Privacy Notices, covering its routine collection of staff, student and third party data. All staff, students and others acting on the University's behalf must comply with the standard Privacy Notices when they collect or Process relevant data. **The standard Privacy Notices are available from the Data Protection Officer, or online here:**

https://www.chi.ac.uk/about-us/policies-and-statements/data-protection

7. PURPOSE LIMITATION

7.1 Personal Data must be collected only for specified, explicit and legitimate purposes. It must not be further Processed in any manner incompatible with those purposes.

7.2 You cannot use Personal Data for new, different or incompatible purposes from that disclosed when it was first obtained unless you have informed the Data Subject of the new purposes and they have provided Consent where necessary.

8. DATA MINIMISATION

8.1 Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed.

8.2 You may only Process Personal Data when required to do so by your work for the University. You cannot Process Personal Data for any other reason.

8.3 Do not collect excessive data. Ensure any Personal Data collected is adequate and relevant for the intended purposes.

8.4 You must ensure that when Personal Data is no longer needed for specified purposes, it is deleted or anonymised in accordance with the University's data retention practices.

9. ACCURACY

9.1 Personal Data must be accurate and, where appropriate, kept up to date. It must be corrected or deleted without delay when inaccurate.

9.2 You must ensure that the Personal Data you use and hold is accurate, complete, kept up to date and relevant to the purpose for which you collected it. You must check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards. You must take all reasonable steps to destroy or amend inaccurate or out-of-date Personal Data.

10. STORAGE LIMITATION

10.1 Personal Data must not be kept in an identifiable form for longer than is necessary for the purposes for which the data is processed.

10.2 You must not keep Personal Data in a form which permits the identification of the Data Subject for longer than needed for the legitimate business purpose or purposes for which we originally collected it including for the purpose of satisfying any legal, accounting or reporting requirements.

10.3 The University will maintain retention policies and procedures to ensure Personal Data is deleted after a reasonable time for the purposes for which it was being held.

10.4 You will take all reasonable steps to destroy or erase from our systems (physical or electronic) all Personal Data that we no longer require in accordance with all the University's retention policies. This includes requiring third parties to delete such data where applicable.

10.5 You will ensure Data Subjects are informed of the period for which data is stored and how that period is determined in any relevant Privacy Notice.

11. SECURITY, INTEGRITY AND CONFIDENTIALITY

Protecting Personal Data

11.1 Personal Data must be secured by appropriate technical and organisational measures against unauthorised or unlawful Processing, and against accidental loss, destruction or damage.

11.2 We will develop, implement and maintain safeguards appropriate to our size, scope and business, our available resources, the amount of Personal Data that we own or maintain on behalf of others and identified risks (including use of encryption and Pseudonymisation where applicable). We will regularly evaluate and test the effectiveness of those safeguards to ensure security of our Processing of Personal Data. You are responsible for protecting the Personal Data we hold. You must implement reasonable and appropriate security measures against unlawful or unauthorised Processing of Personal Data and against the accidental loss of, or damage to, Personal Data. You must exercise particular care in protecting Special Categories of Personal Data from loss and unauthorised access, use or disclosure.

11.3 You must follow all procedures and technologies we put in place to maintain the security of all Personal Data from the point of collection to the point of destruction. You may only transfer Personal Data to third-party service providers who agree to comply with the required policies and procedures and who agree to put adequate measures in place, as requested.

11.4 You must maintain data security by protecting the confidentiality, integrity and availability of the Personal Data, defined as follows:

11.4.1 Confidentiality means that only people who have a need to know and are authorised to use the Personal Data can access it.

11.4.2 Integrity means that Personal Data is accurate and suitable for the purpose for which it is processed.

11.4.3 Availability means that authorised users are able to access the Personal Data when they need it for authorised purposes.

11.5 You must comply with and not attempt to circumvent the administrative, physical and technical safeguards we implement and maintain to protect Personal Data.

Reporting a Data Breach

11.6 The applicable data protection legislation requires all organisations to report certain types of data breach to the relevant supervisory authority within 72 hours, and in some cases to the Data Subjects individuals affected.

11.7 We have put in place procedures to deal with any suspected Data Breach and will notify Data Subjects or any applicable regulator where we are legally required to do so.

11.8 If you know or suspect that a Data Breach has occurred, do not attempt to investigate the matter yourself. Immediately contact the DPO, or if the DPO is unavailable, the University Solicitor, and follow the Data Security Breach Management Process. You should preserve all evidence relating to the potential Data Breach.

12. TRANSFER LIMITATION

12.1 The applicable data protection legislation restricts data transfers to countries outside the EEA in order to ensure that the level of data protection afforded to individuals is not undermined. You transfer Personal Data originating in one country across borders when you transmit, send, view or access that data in or to a different country.

12.2 You may only transfer Personal Data outside the EEA if one of the following conditions applies:

12.2.1 the European Commission has issued a decision confirming that the country to which we transfer the Personal Data ensures an adequate level of protection for the Data Subjects' rights and freedoms (see http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm);

12.2.2 appropriate safeguards are in place (such as appropriate contractual clauses) and have been approved by the DPO and the University Solicitor;

12.2.3 the Data Subject has provided explicit Consent to the proposed transfer after being informed of any potential risks; or

12.2.4 the transfer is permitted for one of the other reasons set out in the applicable data protection legislation.

13. DATA SUBJECT'S RIGHTS AND REQUESTS

13.1 Data Subjects have rights when it comes to how we handle their Personal Data. These include rights to:

13.1.1 withdraw Consent to Processing at any time;

13.1.2 receive certain information about the Data Controller's Processing activities;

13.1.3 request access to their Personal Data that we hold;

13.1.4 prevent our use of their Personal Data for direct marketing purposes;

13.1.5 ask us to erase Personal Data if it is no longer necessary in relation to the purposes for which it was collected or Processed or to rectify inaccurate data or to complete incomplete data;

13.1.6 restrict Processing in specific circumstances;

13.1.7 challenge Processing which has been justified on the basis of our legitimate interests, in the public interest or in fulfilment of a public task;

13.1.8 request a copy of any agreement under which Personal Data is transferred outside of the EEA;

13.1.9 object to decisions based solely on Automated Processing, including profiling (ADM);

13.1.10 prevent Processing that is likely to cause damage or distress to the Data Subject or anyone else;

13.1.11 be notified of a Data Breach which is likely to result in high risk to their rights and freedoms;

13.1.12 make a complaint to the Information Commissioner's Office, or any equivalent or replacement regulatory body having jurisdiction; and

13.1.13 in limited circumstances, receive or ask for their Personal Data to be transferred to a third party in a structured, commonly used and machine readable format.

13.2 If an individual requests information or changes from you under any of the rights listed above, do not take action or disclose data yourself; immediately forward any such request to the DPO. Do not allow

the Data Subject or third parties (such as parents, or the police) to persuade you into disclosing Personal Data without proper authorisation.

14. ACCOUNTABILITY

14.1 The University, as Data Controller, must implement appropriate technical and organisational measures in an effective manner, to ensure compliance with data protection principles. The University is responsible for, and must be able to demonstrate, compliance with the data protection principles.

14.2 The University must have adequate resources and controls in place to ensure and to document compliance including:

14.2.1 appointing and maintaining a suitably qualified DPO role and appropriate management accountability for data privacy;

14.2.2 implementing Privacy by Design when Processing Personal Data and completing DPIAs where Processing presents a high risk to rights and freedoms of Data Subjects;

14.2.3 integrating data protection into internal documents including this Privacy Standard, Privacy Notices and any related documents;

14.2.4 regularly training University staff and, as appropriate, students and sub-contractors, on the applicable data protection legislation, this Privacy Standard and data protection matters including, for example, Data Subject's rights, Consent, legal basis, DPIA and Data Breaches; and

14.2.5 regularly testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance, including using results of testing to demonstrate compliance improvement effort.

Record keeping

14.3 The applicable data protection legislation requires us to keep full and accurate records of all our data Processing activities.

14.4 You must keep and maintain accurate corporate records reflecting our Processing including records of Data Subjects' Consents and procedures for obtaining Consents.

14.5 These records should include, at a minimum, the name and contact details of the Data Controller and the DPO, clear descriptions of the Personal Data types, Data Subject types, Processing activities, Processing purposes, legal bases for processing, third-party recipients of the Personal Data, Personal Data storage locations, Personal Data transfers, the Personal Data's retention period and a description of the security measures in place. In order to create such records, data maps should be created which should include the detail set out above together with appropriate data flows.

Training and audit

14.6 We are required to ensure all University staff and, as appropriate, students and sub-contractors have undergone adequate training to enable them to comply with applicable data protection legislation. We must also regularly test our systems and processes to assess compliance.

14.7 You must undergo all data privacy related training when instructed to do so.

14.8 You must regularly review all the systems and processes under your control to ensure they comply with this Privacy Standard and check that adequate governance controls and resources are in place to ensure proper use and protection of Personal Data.

15. PRIVACY BY DESIGN AND DEFAULT DATA PROTECTION IMPACT ASSESSMENT (DPIA)

15.1 We are required to implement Privacy by Design and Default measures when Processing Personal Data. Systems should be designed such that, by default, privacy is prioritised by implementing appropriate technical and organisational measures (like Pseudonymisation) in an effective manner, to ensure compliance with data privacy principles.

15.2 You must assess what Privacy by Design and Default measures can be implemented on all programs/systems/processes that Process Personal Data by taking into account the following:

15.2.1 the state of the art;

15.2.2 the cost of implementation;

15.2.3 the nature, scope, context and purposes of Processing; and

15.2.4 the risks of varying likelihood and severity for rights and freedoms of Data Subjects posed by the Processing.

16. DATA PROTECTION IMPACT ASSESSMENTS

16.1 Data controllers must conduct DPIAs wherever Processing is deemed to be high risk.

16.2 You should conduct a DPIA (and lodge a copy and discuss your findings with the DPO) when implementing major system or business change programs involving the Processing of Personal Data including:

16.2.1 use of new technologies (programs, systems or processes), or changing technologies;

16.2.2 Automated Processing and ADM;

16.2.3 large scale Processing of Special Categories of Personal Data; and

16.2.4 large scale, systematic monitoring of a publicly accessible area.

16.3 A DPIA must be in the University's standard form and include:

16.3.1 a description of the Processing, its purposes and the legal basis for Processing;

16.3.2 an assessment of the necessity and proportionality of the Processing in relation to its purpose;

16.3.3 an assessment of the risk to individuals; and

16.3.4 the risk mitigation measures in place and demonstration of compliance.

17. AUTOMATED PROCESSING AND AUTOMATED DECISION-MAKING

17.1 **Automated Decision-Making** (ADM) is when a decision is made which is based solely on Automated Processing which produces legal effects or significantly affects an individual. The applicable data protection legislation prohibits Automated Decision-Making (unless certain conditions are met) but not Automated Processing.

17.2 **Automated Processing** is any form of automated processing of Personal Data consisting of the use of Personal Data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Profiling is an example of Automated Processing.

17.3 ADM is prohibited when a decision has a legal or similar significant effect on an individual unless:

17.3.1 a Data Subject has Explicitly Consented;

17.3.2 the Processing is authorised by law; or

17.3.3 the Processing is necessary for the performance of or entering into a contract.

17.4 Where some Special Categories of Personal Data are being processed, then grounds 17.3.2 and 17.3.3 will not apply.

17.5 If a decision is to be based solely on Automated Processing, then Data Subjects must be informed when you first communicate with them of their right to object. This right must be explicitly brought to their attention and presented clearly and separately from other information. Further, suitable measures must be put in place to safeguard the Data Subject's rights and freedoms and legitimate interests.

17.6 We must also inform the Data Subject of the logic involved in the decision making or profiling, the significance and envisaged consequences and give the Data Subject the right to request human intervention, express their point of view or challenge the decision.

17.7 The DPO must be informed, and a DPIA must be carried out, before any Automated Processing or ADM activities are undertaken.

18. DIRECT MARKETING

18.1 We are subject to certain rules and privacy laws when marketing to potential students and other customers of the University.

18.2 For example, a Data Subject's prior consent is required for electronic direct marketing (for example, by email, text or automated calls). The limited exception for existing customers known as "soft opt in" allows organisations to send marketing texts or emails if they have obtained contact details in the course of a sale to that person, they are marketing similar products or services, and they gave the person an opportunity to opt out of marketing when first collecting the details and in every subsequent message.

18.3 The right to object to direct marketing must be explicitly offered to the Data Subject in an intelligible manner so that it is clearly distinguishable from other information.

18.4 A Data Subject's objection to direct marketing must be promptly honoured. Following an opt-out, their details should be suppressed as soon as possible. 'Suppression' involves retaining just enough information to ensure that marketing preferences are respected in the future.

19. SHARING PERSONAL DATA

19.1 Generally we are not allowed to share Personal Data with third parties unless certain safeguards and contractual arrangements have been put in place.

19.2 You may only share the Personal Data we hold with another staff member, student, or other representative of the University if the recipient has a need to know the information and the transfer complies with any applicable cross-border transfer restrictions.

19.3 You may only share the Personal Data we hold with third parties, such as our service providers, if:

19.3.1 they have a need to know the information for the purposes of providing the contracted services;

19.3.2 sharing the Personal Data complies with the Privacy Notice provided to the Data Subject and, if required, the Data Subject's Consent has been obtained;

19.3.3 the third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place;

19.3.4 the transfer complies with any applicable cross border transfer restrictions; and

19.3.5 a fully executed written contract that contains University Solicitor-approved third party clauses has been obtained.

20. CHANGES TO THIS PRIVACY STANDARD

20.1 We reserve the right to change this Privacy Standard at any time. Please check back regularly to obtain the latest copy of this Privacy Standard.

20.2 This Privacy Standard does not override the applicable data protection legislation or any applicable national data privacy laws and regulations in countries where the University operates.