**CANTERBURY CHRIST CHURCH UNIVERSITY**

**DATA PROTECTION POLICY**

Canterbury Christ Church University is committed to protecting all data we handle about people we support and work with, and to respecting people’s rights around how their information is handled.

*Our responsibilities extend to the personal data of any individual about whom we collect data for any purpose. These responsibilities are not just about data about staff and students; it extends to anyone with whom the University has contact. All employees, including volunteers, temporary and contract staff, have responsibilities under this policy.*

This policy explains our responsibilities and how we will meet them. There has been a revision of the policy to take account of changes in data protection law that came into effect on 25 May 2018.

Before you collect or handle any personal data as part of your work for the University, it is important you take the time to read this policy carefully and understand what is required of you, as well as the organisation’s responsibilities when we process data.

***Any questions and queries can be addressed to the University’s Data Protection Officer at*** [***dp.officer@canterbury.ac.uk***](mailto:dp.officer@canterbury.ac.uk)***.***

*There is an on-line guide for staff available at:* [*https://cccu.canterbury.ac.uk/governance-and-legal-services/the-general-data-protection-regulation/the-general-data-protection-regulation.aspx*](https://cccu.canterbury.ac.uk/governance-and-legal-services/the-general-data-protection-regulation/the-general-data-protection-regulation.aspx)

Adopted: 22 May 2018

## **Contents**

Section A – What this policy is for 3

1. Policy statement 3

2. Why this policy is important 4

3. How this policy applies to you and what you need to know 4

4. Training and guidance 5

Section B – The University’s data protection responsibilities 5

5. What personal data does the University process? 5

6. Making sure processing personal data is fair and lawful 6

How can the University legally use personal data? 6

How can the University legally use special categories of data? 7

What must the University tell data subjects before we use their personal data? 7

7. When the University needs consent to process personal data 8

8. Processing for specified purposes 8

9. Data will be adequate, relevant and not excessive 8

10. Accurate data 9

11. Keeping data and destroying it 9

12. Security of personal data 9

13. Keeping records of our data processing 9

Section C – Working with people the University processes data about data subjects 10

14. Data subjects’ rights 10

15. Direct marketing 10

Section D – working with other organisations and transferring data 11

16. Sharing information with a third party (other organisations or individuals) 11

17. Data processors 12

18. Transferring personal data outside the European Union (EU) 12

Section E – Managing change and risks 12

19. Data protection impact assessments 12

20. Dealing with data protection breaches 13

Schedule 1 – Definitions 14

# Section A – What this policy is for

# Policy statement

* 1. Canterbury Christ Church University is the data controller in relation to the processing activities described below. This means the University decides why and how your personal information is processed.
  2. The University revised the Data Protection Policy to take account of the changes in data protection law, particularly the General Data Protection Regulation (GDPR) and the Data Protection Act [2018].
  3. *A glossary of key terms is provided in Schedule 1 at the end of this document*
  4. Where this policy refers to “we”, “our” or “us” below, unless it mentions otherwise, it is referring to Canterbury Christ Church University.

## We are committed to protecting personal data and respecting the rights of our **data subjects**, who are the people whose **personal data** we collect and use. We value the personal data entrusted to us and respect that trust, by complying with the Data Protection Act and General Data Protection Directive, and adopting best practice promoted by the Information Commissioners Office (ICO).

## The University processes personal information for a range of contractual, statutory or public interest purposes, including the following:

## provide, deliver and administer education

## provide administrative and support services to our students and staff

## advertise and promote the University and the services we offer

## undertake research (including research relating to health)

## undertake fundraising

### provide commercial activities to clients

### recruit, support and manage staff, agents, contractors and students

### manage the records of our students, staff and contracted personnel

### maintain relations with business contacts, suppliers, professional advisers and consultants

### maintain relations with landlords and tenants

### maintain relations with donors and alumni

### maintain relations with health, welfare, government and social organisations

### provide pastoral support for students and staff;

### provide services to the community

### safeguard children, young people and adults at risk

### maintain our accounts and records

### maintain the security of property and premises

### respond effectively to enquirers and handle any complaints, and requests about persons who may be the subject of enquiry

### maintain relations with authors, publishers and other creators

### manage data relating to individuals captured by CCTV images, and collect visual images for the purposes of security and the prevention and detection of crime

### provide references

## This policy has been approved by the Senior Management Team. It sets out the legal rules that apply whenever we obtain, store or use personal data.

# Why this policy is important

## The University has a commitment to protecting personal data from being misused for example getting into the wrong hands as a result of poor security or being shared carelessly, or being inaccurate. The ICO can take regulatory action, including imposing fines, if the University misuses data. In addition, there are reputational risks arising from misuse, and it can cause upset or distress to individuals.

## This policy sets out the measures the University are committed to taking and what every member of staff at the University, including volunteers, temporary and contract staff, will do to ensure we comply with the relevant legislation.

## In particular, we will make sure that all personal data is:

### processed **lawfully, fairly and in a transparent manner**;

### processed for **specified, explicit and lawful purposes**, set out in Section 6, and not in a manner that is incompatible with those purposes;

### **adequate, relevant and limited to what is necessary** for the purposes for which it is being processed;

### **accurate** and, where necessary, up to date;

### **not kept longer than necessary** for the purposes for which it is being processed;

### processed in a **secure** manner, by using appropriate technical and organisational means;

### processed in keeping with the **rights of data subjects** regarding their personal data.

# How this policy applies to you and what you need to know

## Below outlines how the Policy applies to each key group involved in the provision, collection and use of personal data for the University:

## **As an employee or volunteer** processing personal information on behalf of the University, you are required to comply with this policy. If you think you – or another employee - breached the policy, even by accident, it is important you contact our Data Protection Officer immediately. This is so we can take swift action to try and limit the impact of the breach.

## Anyone who intentionally or recklessly breaches the Data Protection Policy may be subject to disciplinary action. In certain circumstances, the individual may also be liable to criminal prosecution, including by the ICO.

## **As a manager** you are required to ensure that any procedures that involve personal data, that you are responsible forin your area, follow the rules set out in this Data Protection Policy.

## **As a data subject, the University** will handle your personal information in line with this policy.

## **Any company appointed as a data processor/contractor is required** to comply with the University’s Data Protection Policy under their contract with it. Any breach of the policy will be taken seriously and could lead to us taking contract enforcement action against the company, or terminating the contract. Data processors have direct obligations under the GDPR, primarily to only process data on instructions from the University and to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk involved.

## **The University’s Data Protection Officer** is responsible for advising the University and its staff and members about their legal obligations under data protection law, monitoring compliance with data protection law, dealing with data security breaches and with the development of the Data Protection Policy. Any questions about this policy or any concerns that the policy has not been followed should be referred to them at dp.officer@canterbury.ac.uk.

## Our procedures will be in line with the requirements of this policy, but if you are unsure about whether anything you plan to do, or are currently doing, might breach this policy you should contact the Data Protection Officer.

# Training and guidance

## The University will provide online training, which all staff should undertake at least annually to raise awareness of their obligations and the University’s responsibilities, as well as to outline the law. This includes volunteers, temporary and contract staff.

## The University will also arrange face-to-face training with relevant staff on specific aspects of compliance with data protection law, as required.

## The University will issue procedures, guidance or instructions from time to time. Managers must set aside time for their team to look together at the implications for their work.

# Section B – The University’s data protection responsibilities

# What personal data does the University process?

## In the course of the University’s work, it may collect and process information (personal data) about many different people (data subjects). This includes data it receives straight from the data subject, for example, where they complete forms or contact the University. The University may also receive information about data subjects from other sources including, for example, previous employers and UCAS.

## The University processes personal data in both electronic and paper form. All this data is protected under data protection law. The personal data it processes can include information such as names and contact details, education or employment details, email, voice mail and visual images of people.

## In some cases, the University holds types of information that are called **“special categories”** of data in the GDPR. This personal data can only be processed under strict conditions.

## **‘Special categories’ of data** consists of information about a person’s:

## racial or ethnic origin;

## political opinions;

## religious or similar (e.g. philosophical) beliefs;

## trade union membership;

## health (including physical and mental health, and the provision of health care services);

## genetic data;

## biometric data;

## sexual life and sexual orientation.

## The University will not hold information relating to criminal proceedings or offences or allegations of offences. The exceptions are where there is an overarching safeguarding requirement to process this data for the protection of children and vulnerable adults who may be put at risk through the activities of the University and for the purposes of taking disciplinary action.

## Other data may also be considered ‘sensitive’ such as bank details, and whilst these will need to be subject to appropriate safeguards, it will not be subject to the same legal protection as the types of data listed above.

# Making sure processing personal data is fair and lawful

## Processing of personal data will only be fair and lawful when the purpose for the processing meets a legal basis, as listed below, and when the processing is transparent. This means the University will provide people at the point of collection with an explanation of how and why it processes their personal data at the point it collects data from them, as well as when it collects data about them from other sources.

# How can the University legally use personal data?

## Processing of personal data is only lawful if at least one of these legal conditions, as listed in Article 6 of the GDPR, is met:

### the processing is **necessary for a contract** with the data subject;

### the processing is **necessary for us to comply with a legal obligation**;

### the processing is necessary to protect someone’s life (this is called “**vital interests**”);

### the processing is necessary for us to perform a task in the **public interest**, and the task has a clear basis in law;

### the processing is **necessary for legitimate interests** pursued by the Universityor another organisation, unless these are overridden by the interests, rights and freedoms of the data subject.

### If none of the other legal conditions apply, the processing will only be lawful if the data subject has given their **explicit written consent**.

# How can the University legally use special categories of data?

## Processing of special categories of personal data is only lawful when, in addition to the conditions above, one of the extra conditions, as listed in Article 9 of the GDPR, is met. These extra conditions include where:

### the processing is necessary for **carrying out our obligations under employment and social security and social protection law**;

### the processing is necessary for **safeguarding the vital interests** (in emergency, life or death situations) **of an individual** and the data subject is incapable of giving consent;

### the processing is necessary for reasons of public interest in the area of **public health;**

### the processing is necessary for the purposes of **preventive or occupational medicine**, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services;

### the processing is necessary for **pursuing legal claims**.

### The processing is necessary for **archiving purposes** in the public interest, scientific or historical research purposes or statistical purposes

### If none of the other legal conditions apply, the processing will only be lawful if the data subject has given their **explicit** **written** **consent**.

## Before deciding which condition should be relied upon, the University may refer to the original text of the GDPR as well as any relevant guidance.

# What must the University tell data subjects before we use their personal data?

## If personal data is collected directly from the individual, we will inform them about;

## the full name and address of the University, and those of the University’s Data Protection Officer;

## the reasons for processing, and the legal bases, (including explaining any automated decision-making or profiling, explaining the legal basis for collecting the data, and explaining, where relevant, the consequences of not providing data needed for a contract or statutory requirement);

## who we will share the personal data with;

## if we plan to send the personal data outside of the European Union (EU);

## how long we will store the personal data; and

## the data subjects’ rights.

### This information is referred to as a ‘Privacy Notice’. This information needs to be given at the time when the personal data is collected.

## If data is collected from another source, rather than directly from the data subject, the University will provide the data subject with the information described in section 6.5 as well as:

## the categories of the data concerned; *and*

## the source of the data.

## This information will be provided to the data subject in writing and no later than within **1 calendar month** after the University receives the data, unless a legal exemption under the GDPR applies. If the University uses the data to communicate with the data subject, it will at the latest give them this information at the time of the first communication.

## If the University plans to transfer data onto outside of the University, it will notify the data subject before it passes on the data, for instance in a privacy notice, unless the transfer is subject to an exemption under the Data Protection Act 2018.

# When the University needs consent to process personal data

## Where none of the other legal conditions apply to the processing, and the University is required to get consent in writing from the data subject. We will clearly set out the reason for asking consent, including why we are collecting the data and how we plan to use it. Consent will be specific to each process for which we request consent for. The University will only ask for consent when the data subject has a real choice whether or not to provide us with their data.

## The data subject can withdraw consent at any time, by any means. If withdrawn, the University will stop processing the data. Data subjects will be informed of their right to withdraw consent. It will be as easy to withdraw consent as it is to give consent.

# Processing for specified purposes

## The University will only process personal data for the specific purposes explained in its privacy notices (as described above in section 6.5) or for other purposes specifically permitted by law. It will explain those other purposes to data subjects in the way described in section 6, unless there are lawful reasons for not doing so.

# Data will be adequate, relevant and not excessive

## The University will only collect and use personal data that is needed for the specific purposes described above (which will normally be explained to the data subjects in privacy notices). It will not collect more than is needed to achieve those purposes. It will not collect any personal data “just in case” it wants to process it later.

# Accurate data

## The University will make sure that personal data held is accurate and, where appropriate, kept up to date. The accuracy of personal data will be checked at the point of collection and at appropriate points later on.

# Keeping data and destroying it

## The University will not keep personal data longer than is necessary for the purposes that it was collected for.

## Information about how long the University will keep records for can be found in its Information Asset Register.

# Security of personal data

## The University will use appropriate measures to keep personal data secure at all points of the processing. Keeping data secure includes protecting it from unauthorised or unlawful processing, or from accidental loss, destruction or damage.

## We will implement security measures which provide a level of security which is appropriate to the risks involved in the processing.

## Measures will include technical and organisational security measures. In assessing what measures are the most appropriate the University will take into account the following, and anything else that is relevant:

### the quality of the security measure;

### the costs of implementation;

### the nature, scope, context and purpose of processing;

### the risk (of varying likelihood and severity) to the rights and freedoms of data subjects;

### the risk which could result from a data breach.

## Measures include:

### technical systems security;

### measures to restrict or minimise access to data;

### measures to ensure its systems and data remain available, or can be easily restored in the case of an incident;

### physical security of information and of its premises;

### organisational measures, including policies, procedures, training and audits;

### regular testing and evaluating of the effectiveness of security measures.

# Keeping records of our data processing

## To show how the University complies with the law we will keep clear records of our processing activities and of the decisions we make concerning personal data setting out our reasons for those decisions.

## All employees are responsible for producing clear records. The University provides advice on who is responsible for maintaining these records of processing activities.

# Section C – Working with people the University processes data about data subjects

# Data subjects’ rights

## The University will process personal data in line with data subjects' rights, including their right to:

### request access to any of their personal data held by us (known as a Subject Access Request);

### ask to have inaccurate personal data changed;

### restrict processing, in certain circumstances set out in Article 18 of the GDPR;

### object to processing, including preventing the use of their data for direct marketing, unless the University demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims;

### data portability, which means to receive their data, or some of their data, in a format that can be easily used by another person (including the data subject themselves) or organisation;

### not be subject to automated decisions, in certain circumstances set out in Article 22 of the GDPR; and

### withdraw consent when we rely on consent to process their data.

## If a member of staff receives any request from a data subject that relates or could relate to their data protection rights, this must be forwarded to the Data Protection Officer **immediately**.

## The University will act on all valid requests as soon as possible, and at the latest within **one calendar month**, unless we have reason to, and can lawfully extend the timescale. This can be extended by up to two months in certain circumstances defined in the GDPR.

## All data subjects’ rights are provided free of charge.

## Any information provided to data subjects should be concise and transparent, using clear and plain language.

# Direct marketing

## The University will comply with the rules set out in the GDPR, the Privacy and Electronic Communications Regulations (PECR) and any laws which may amend or replace the regulations around **direct marketing**. This includes, but is not limited to, when it makes contact with data subjects by post, email, text message, social media messaging, telephone (both live and recorded calls) and fax.

## **Direct marketing** means the communication (by any means) of any advertising or marketing material which is directed, or addressed, to individuals.“Marketing” does not need to be selling anything, or be advertising a commercial product. It includes contact made by organisations to individuals for the purposes of promoting the organisation’s aims.

## Any direct marketing material will identify the University as the sender and will describe how people can object to receiving similar communications in the future. If a data subject exercises their right to object, by any means, to direct marketing the University will stop the direct marketing as soon as possible.

# Section D – working with other organisations and transferring data

# Sharing information with a third party (other organisations or individuals)

## The University sometimes needs to share the personal data it processes with a third party, either another individual or another organisations. Where this is necessary the University must comply with all aspects of data protection legislation.

## The University will only share personal data with other organisations or third party individuals when we have a legal basis to do so (including explicit written consent) and informed the data subject about the possibility of the data being shared in a privacy notice. The exception is where there are legal exemptions which do not require us to inform the data subject about the data sharing.

## What follows is an indicative description of the types of third parties the University may need to share some of the personal data it processes with for one or more reasons, where necessary:

## representatives of the person whose personal data we are processing

## providers of placements as part of a student’s course

## partner institutions where a student is studying the whole or part of a course

## current, past or prospective employers

## healthcare, social and welfare organisations

## educators and examining bodies

## suppliers and service providers

## the Students’ Union

## financial organisations

## debt collection and tracing agencies

## auditors

## police forces and security organisations

## courts and tribunals

## prison and the probation services

## legal representatives

## local and central government

## consultants and professional advisers

## trade union and staff associations

## survey and research organisations

## press and the media

## voluntary and charitable organisations

## landlords

## authors, publishers and other creators

## persons who may be the subject of enquiry

## third parties participating in course work

## individuals captured by CCTV images

## volunteers

## witnesses

## parties to legal proceedings and their insurers

## parties to transactions or dispute resolution procedures

## The University will record information shared with a third party, which will include recording any exemptions which have been applied, and why they have been applied. It will follow the ICO’s statutory [***Data Sharing Code of Practice***](https://ico.org.uk/media/for-organisations/.../data_sharing_code_of_practice.pdf) (or any replacement code of practice) when sharing personal data.

# Data processors

## Before appointing a contractor who will process personal data on the University’s behalf (a data processor) the University will carry out due diligence checks. The checks are to make sure the processor will use appropriate technical and organisational measures to ensure the processing will comply with data protection law, including keeping the data secure, and upholding the rights of data subjects. The University will only appoint data processors who can provide us with sufficient guarantees that they will do this.

## The University will only appoint data processors on the basis of a written contract that will require the processor to comply with all relevant legal requirements. The University will continue to monitor the data processing, and compliance with the contract, throughout the duration of the contract.

# Transferring personal data outside the European Union (EU)

## It may sometimes be necessary to transfer personal data overseas. When this is needed data may be transferred to countries or territories around the world.

## Personal data cannot be transferred (or stored) outside of the European Union (EU) unless this is permitted by the GDPR. This includes storage on a “cloud” based service where the servers are located outside the EU.

## The University will only transfer data outside the EU where it is permitted by one of the conditions for non-EU transfers in the GDPR.

# Section E – Managing change and risks

# Data protection impact assessments

## When the University are planning to carry out any data processing which is likely to result in a high risk it will carry out a Data Protection Impact Assessment (DPIA). These include situations when the University processes data relating to vulnerable people, trawling of data from public profiles, using new technology, and transferring data outside the EU. Any decision not to conduct a DPIA will be recorded, including setting out the reason.

## The University may also conduct a DPIA in other cases when it considers it appropriate to do so. If the University is unable to mitigate the identified risks such that a high risk remains, it will consult with the ICO.

## DPIAs will be conducted in accordance with the ICO’s Code of Practice ‘[Conducting privacy impact assessments](https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf)’.

# Dealing with data protection breaches

## Where staff or volunteers, or contractors working for the University, think that this policy has not been followed, or data might have been breached or lost, this must be reported **immediately** to the Data Protection Officer.

## The University will keep records of all personal data breaches, even if it is determined the breach does not fulfil the criteria for reporting to the ICO.

## The University, through the Data Protection Officer or nominee, will report all data breaches which are likely to result in a risk to any data subject, to the ICO. Reports are to be made to the ICO within **72 hours** from when any person in the University becomes aware of the breach.

## In situations where a personal data breach causes a high risk to any data subject, the University will (as well as reporting the breach to the ICO), inform data subjects whose information is affected, without undue delay. This can include situations where, for example, bank account details are lost or an email containing sensitive information is sent to the wrong recipient. Informing data subjects can enable them to take steps to protect themselves and/or to exercise their rights.

# Schedule 1 – Definitions

## The following terms are used throughout the University’s Data Protection Policy and have their legal meaning as set out within the GDPR. The GDPR definitions are further explained below:

## **Automated decision taking** results in decisions taken (a) using personal data processed solely by automatic means and (b) having a significant effect on the individual concerned.

## **Data controller** means any person, company, authority or other body who (or which) determines the means for processing personal data and the purposes for which it is processed. It does not matter if the decisions are made alone or jointly with others.

## The data controller is responsible for the personal data which is processed and the way in which it is processed. The University are the data controller of data which it processes.

## **Data processors** include any individuals or organisations, which process personal data on the University’s behalf and on its instructions e.g. an external organisation which provides secure waste disposal for the University. This definition will include the data processors’ own staff (note that staff of data processors may also be data subjects).

## **Data subjects** include all living individuals who the University holds or otherwise processes personal data about. A data subject does not need to be a UK national or resident. All data subjects have legal rights in relation to their personal data. Data subjects that the University are likely to hold personal data about include:

### students

### alumni

### employees (and former employees) and contracted personnel

### suppliers, professional advisers and consultants, including individuals who are the University’s contractors or employees working for them

### business contacts

### landlords or tenants

### volunteers

### complainants

### supporters

### enquirers

### friends and family of staff and students

### advisers and representatives of other organisations.

### donors and alumni

### authors, publishers and other creators

### persons who may be the subject of enquiry

### third parties participating in course work

### health, welfare, government and social organisations

### individuals captured by CCTV images

### clients

### witnesses

### parties to legal proceedings

### parties to transactions or dispute resolution procedures

## **ICO** means the Information Commissioner’s Office which is the UK’s regulatory body responsible for ensuring that the University complies with its legal data protection duties. The ICO produces guidance on how to implement data protection law and can take regulatory action where a breach occurs.

## **Personal data** means any information relating to a natural living person who is either identified or is identifiable. It is the information from which a living person can be identified or is identifiable. A natural person must be an individual and cannot be a company or a public body, although representatives of companies or public bodies would be natural persons.

## Personal data is limited to information about living individuals and does not cover deceased people.

## Personal data can be factual (for example, a name, address or date of birth) or it can be an opinion about that person, their actions or behaviour.

## **Privacy notice** means the information given to data subjects which explains how the University processes their data and for what purposes.

## **Processing** is very widely defined and includes any activity that involves the data. It includes obtaining, recording, holding, storage and disposing the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing can also include transferring personal data to third parties, listening to a recorded message (e.g. on voicemail) or viewing personal data on a screen or in a paper document which forms part of a structured filing system. Viewing of clear, moving or stills images of living individuals is also a processing activity.

## **Special categories of data** (as identified in the GDPR) includes information about a person’s:

### Racial or ethnic origin;

### Political opinions;

### Religious or similar (e.g. philosophical) beliefs;

### Trade union membership;

### Health (including physical and mental health, and the provision of health care services);

### Genetic data;

### Biometric data;

### Sexual life and sexual orientation.