Canterbury Christ Church University

Data Protection Policy

Approved by:	Effective date:	Next review:
Information Governance Group	November 2025	November 2027

Policy statement

The Data Protection Policy provides a framework to ensure the University meets its obligations under the UK General Data Protection Regulation and the Data Protection Act 2018.

Who needs to know about the policy?

- Staff, including contractors and Associates
- Students
- Applicants
- Customers

Purpose of the policy

The University sets out how it is to comply with data protection legislation guided by the six data protection principles, which require that personal data is:

- Processed fairly, lawfully and in a transparent manner.
- Used only for limited, specified stated purposes and not used or disclosed in any way incompatible with those purposes.
- Adequate, relevant, and limited to what is necessary.
- Accurate and, where necessary, up to date.
- Not kept for longer than necessary; and
- Kept safe and secure.

In addition, the accountability principle requires us to evidence our compliance with the above six principles and ensure we do not put individuals at risk because of processing their data. Failure to do so can result in a breach of legislation, reputational damage, or financial implications due to fines. To meet our obligations, we put in place appropriate and effective measures to comply with data protection law.

The Policy sets out the measures the University is committed to taking and what every staff member at the University will do to ensure compliance with the relevant legislation.

Contacts

Staff have access to supporting policies, operational procedures and guidance which is available on the intranet.

The Data Protection Officer is responsible for the following:

- Providing advice and assistance to all members of staff
- Providing appropriate guidance on the implementation of the Policy

- Ensuring the provision of appropriate training

You can refer any questions about this Policy or concerns arising from it to the Data Protection

Officer. The Data Protection Officer can be contacted by emailing: dp.officer@canterbury.ac.uk

Canterbury Christ Church University

Data Protection Policy

Contents

1. Information covered by Data Protection Legislation

1.1. Canterbury Christ Church University is the data controller concerning the processing activities described below. Where this Policy refers to "we", "our", or "us" below, unless it mentions otherwise, it is referring to Canterbury Christ Church University.

1.2. The University decides why and how personal information is processed. It is registered with the Information Commissioner's Office (ICO). The registration number is Z7043317.

1.3. There is a glossary of key terms in Schedule 1 at the end of this document.

1.4. The UK GDPR definition of "personal data" includes any information about an identified or identifiable natural living person.

2. Our Commitment

2.1. The University is committed to transparent, lawful, and fair proportionate processing of personal data. It includes all personal data we process about students, staff or those who work or interact with us.

2.2. The University is committed 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 fines, if the University misuses data. In addition, reputational risks arise from misuse, which can also cause upset or distress to individuals.

2.3. We process data in keeping with the rights of data subjects regarding their data. We value the personal data entrusted to us and respect that trust by complying with the Data Protection Act 2018 (DPA 2018) and UK General Data Protection Directive (UK GDPR) and adopting best practices promoted by the Information Commissioners Office (ICO).

2.4. We will process data according to the data protection principles to ensure the following:

1. Data are processed lawfully, fairly and in a transparent manner.
2. Data are processed for specified, explicit and lawful purposes, set out in Section 6, and not in a manner incompatible with those purposes.
3. There are adequate, relevant limits or controls to what is necessary for processing.
4. Data are accurate and, where necessary, up to date;
5. Data not kept longer than necessary for the processing purpose;
6. Data are processed securely by using appropriate technical and organisational means

3. Roles and Responsibilities

3.1. The University, as a corporate body, is the data controller. All staff are responsible for delivering the University commitment to protecting the rights and privacy of individuals (including students, staff and those who work or interact with us) in processing personal data.

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

3.3. All staff who process personal data must ensure they

1. comply with this Policy
2. undertake regular training to become aware of the requirement for data protection
3. understand their obligations to protect personal data, and follow the guidance provided at all times
4. keep all personal data securely
5. keep data no longer than is necessary for the purpose for which it was collected
6. do not disclose personal data either orally or in writing, accidentally or otherwise, to any unauthorised third party
7. report any breach likely to result in unauthorised disclosure, damage, destruction or loss of Personal Data to the Data Protection Officer immediately and take swift action to try and limit the impact of the breach, and engage in any subsequent enquiries
8. check any information that they process is accurate and up to date, and update changes and correct any errors as soon as possible
9. where there is uncertainty around a data protection matter, seek advice from the Data Protection Officer
10. when supervising students undertaking research with personal data, ensure the students are aware of the Data Protection principles

3.4. Deans and Heads of Schools and Heads of Professional Services are responsible for

1. developing and maintaining good information handling practices following this Policy and the Information Security Policy
2. maintaining accurate records of the data processed in their area
3. ensuring those within their area of responsibility know what data they hold through an appropriate Privacy Notice
4. ensuring their staff are trained in Data Protection and are aware of their responsibilities
5. Ensuring staff undertaking research which involves personal data carry it out following data protection and ethical guidelines.
6. documenting data retention if the processing is unique to their area.

3.5. Managers must ensure that any procedures involving personal data they are responsible for in their area follow the requirements of the Data Protection Policy.

3.6. Information Asset Owners look after each information asset and aid the University in managing personal data and its associated risks.

3.7. The Director of Digital Strategy and Information Technology is responsible for ensuring the security of the University's IT environment for processing personal data. The University achieves this by providing appropriate technical and organisational security measures to protect personal data. The Director is also responsible for maintaining a record of breaches in conjunction with the Information Security Manager.

3.8. The University's Data Protection Officer is responsible for

1. advising the University and its staff and members about their legal obligations under the data protection laws
2. monitoring compliance with data protection law,
3. dealing with data security breaches
4. Implementing the Data Protection Policy.

3.9. 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.

4. Whose Personal Data the University Processes

4.1. The University needs to process personal data to carry out its functions. It 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.

4.2. We may collect and process personal data about people (data subjects). These data subjects include, but are not limited to:

1. Staff concerning their contract of employment
2. Applicants to manage their applications and inform them of study opportunities
3. Students concerning their studies
4. Graduates concerning creating an alumni community and providing information relating to their previous studies
5. Visitors to the University, including those coming to University events
6. Contractors
7. Other third parties with whom it has dealings

5. Why the University Processes Personal Data

5.1. The University needs to collect, store, use, transfer and dispose of data to fulfil its purposes of providing Higher Education and Research. These include undertaking and administering students' education, employing staff and undertaking research. We must meet our legal obligations to regulatory and funding bodies, professional bodies, and the government. For some of these functions, such as teaching, learning and research, the University is acting as a public authority.

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

1. provide, deliver and administer education
2. provide administrative and support services to our students and staff and those who work or interact with us
3. advertise and promote the University and the services we offer
4. undertake research (including research relating to health)
5. undertake fundraising activities
6. provide commercial activities to clients
7. recruit, support and manage staff, agents, contractors and students
8. handle the records of our students, staff and contracted personnel
9. maintain relations with business contacts, suppliers, professional advisers and consultants
10. maintain links with landlords and licensees
11. maintain relations with donors and alumni

12. maintain relations with health, welfare, government and social organisations

13. provide pastoral support for students and staff

14. provide services to the community

15. safeguard children, young people and adults at risk

16. maintain our accounts and records

17. maintain the security of property and premises

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

19. maintain relations with authors, publishers and other creators

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

21. provide references

6. How the University Processes Personal Data

6.1. The University processes personal data in both electronic and paper form. The personal data we process can include information such as names and contact details, education or employment details, email, voice mail and visual images of people.

6.2. The University will only collect and use personal data needed for specific purposes, including those in Section 5. We will not collect more than is required to achieve those purposes or on a “just in case” basis.

6.3. The University will ensure that the personal data held is accurate and, where appropriate, kept up to date. There will be checks on the accuracy of personal data at the point of collection and relevant processing points later on.

6.4. The University will not keep personal data longer than is necessary for its intended use and set out the periods in retention schedules.

7. Making Sure Processing Personal Data is Fair and Lawful

7.1. 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.

7.2. Processing personal data is lawful if at least one of these legal conditions, as listed in Article 6 of the UK GDPR, is met because the processing is necessary

1. for the performance of a contract with the data subject;

2. for us to comply with a legal obligation;

3. for us to perform a task in the public interest, which has a clear basis in law; and

4. for legitimate interests pursued by the University or another organisation unless overridden by the interests, rights and freedoms of the data subject to protect someone's life (this is called "vital interests").

7.3. Where none of the above legal conditions applies to the processing, the University must get consent from the data subject in writing. We will set out the reason for asking for 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. The University will only ask for consent when the data subject has a real choice whether or not to provide us with their data.

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

7.5. The University provides individuals with an explanation of how and why it processes their data before it collects data from them and when it collects data about them from other sources. We do so through the privacy notices published on our website explaining our use of data.

8. Special Category, Criminal and Sensitive Data

8.1. In some cases, the University processes information called special category data in the UK GDPR.

8.2. Special category data consist of information about a person's:

1. racial or ethnic origin;
2. politics;
3. religious or similar (e.g. philosophical) beliefs;
4. trade union membership;
5. health (including physical and mental health and the provision of health care services;
6. genetic data;
7. biometric data;
8. sexual life and sexual orientation.

8.3. The University processes information about criminal proceedings, offences, or allegations where there is an overarching safeguarding requirement to process this data. For example, it processes data to protect children and vulnerable adults who may be put at risk through the activities of the University and to take disciplinary action.

8.4. We process special category and criminal personal data under specific conditions. Processing special categories of personal data is lawful when one of the extra conditions, as listed in Article 9 of the UK GDPR, is met. These additional conditions include where processing is necessary for:

1. carrying out our obligations under employment and social security and social protection law;

2. health or social care purposes, including 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

3. reasons of public interest in the area of public health

4. archiving purposes in the public interest, scientific or historical research purposes or statistical purposes;

5. Substantial public interest, including

- Equality of opportunity or treatment
- Racial and ethnic diversity at senior levels of organisations
- Preventing or detecting unlawful acts
- Protecting the public against dishonesty
- Regulatory requirements relating to unlawful acts and dishonesty
- Support for individuals with a particular disability or medical condition
- Counselling
- Safeguarding children and individuals at risk
- Insurance

8.5. Other data, such as bank details, may also be considered 'sensitive'. While these are subject to appropriate safeguards, they will not be subject to the same legal protection as the data types listed above.

9. Sharing Information with a Third Party (Other Organisations or Individuals)

9.1. The University sometimes needs to share the personal data it processes with a third party, another individual or another organisation. The University complies with all aspects of data protection legislation where this is necessary.

9.2. The following 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:

1. representatives of the person whose personal data we are processing

2. providers of placements as part of a student's course

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

4. current, past or prospective employers

5. healthcare, social and welfare organisations

6. external examiners and examining bodies
7. suppliers and service providers
8. regulatory and statutory bodies
9. the Students' Union
10. financial organisations
11. debt collection and tracing agencies
12. auditors
13. insurers
14. police forces and security organisations
15. courts and tribunals
16. prison and the probation services
17. legal representatives and adjudication services
18. local and central government
19. consultants and professional advisers
20. trade unions and staff associations
21. survey and research organisations
22. press and the media
23. voluntary and charitable organisations
24. landlords
25. authors, publishers and other creators
26. persons who may be the subject of enquiry
27. third parties participating in coursework
28. individuals captured by CCTV images
29. volunteers
30. witnesses
31. parties to legal proceedings and their insurers
32. parties to transactions or dispute resolution procedures

9.3. When we share personal data, we follow the ICO's statutory Data Sharing Code of Practice (or any replacement code of practice).

10. Transferring Personal Data Outside the United Kingdom

10.1. It may sometimes be necessary to transfer personal data overseas. When this is needed, we may transfer data to countries or territories worldwide. The University cannot transfer personal data to other countries unless the UK GDPR permits this. It includes storage on a "cloud" based service on servers outside the EU.

10.2. Data transfer can be transferred when UK adequacy regulations are in place regarding the country where the receiver is located. It includes countries in the European Union.

10.3. The University will only transfer data to other counties where permitted by one of the conditions for non-EU transfers in the UK GDPR. It includes the University putting in place one of the 'appropriate safeguards' referred to in the UK GDPR, such as the International Data Transfer Agreement or Binding Corporate Rules.

11. Security of Personal Data

Organisational and Technical Measures

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

11.2. We will implement security measures that provide a level of security appropriate to the risks involved in the processing.

11.3. 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:

1. the quality of the security measure;
2. the costs of implementation;
3. the nature, scope, context and purpose of the processing;
4. the risk (of varying likelihood and severity) to the rights and freedoms of data subjects;
5. the risk which could result from a data breach.

11.4. Measures include:

1. technical systems security;
2. measures to restrict or minimise access to data;

3. measures to ensure its systems and data remain available or easily restored in the case of an incident;

4. physical security of information and its premises;

5. organisational measures, including policies, procedures, training and audits;

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

Contractors and Data Processing

11.6. Before appointing a contractor who will process personal data on the University's behalf (a data processor), the University will conduct due diligence checks. The checks ensure the processor will use appropriate technical and organisational measures and 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.

11.7. The University will only appoint data processors based on a written contract requiring 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 time it is in force.

11.8. Any company appointed as a data processor/contractor must 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.

11.9. Data processors have direct obligations under the UK 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.

12. Privacy Notices

12.1. A privacy notice sets out the information about why we need people's data, what we plan to do with it, how long we will keep it, and with whom we will share it.

12.2. We seek to explain what we are doing with people's data and ensure they know about it in advance. Being clear helps us build trust, avoids confusion, and lets everyone know what to expect. We provide this information before or when the personal data is collected.

12.3. If data is collected directly from the person, we will inform them about the;

1. the full name and address of the University and those of the University's Data Protection Officer;

2. the reasons for the 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);

3. who we will share the personal data with;

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

5. how long we will store the personal data; and

6. the data subjects' rights.

12.4. Should the data come from somewhere other than the data subject, the University will provide the information described above as well as:

1. the categories of the data concerned; and

2. the source of the data.

13. Data Subjects' Rights

13.1. The University will process personal data in line with data subjects' rights, including their right (subject to permitted restrictions) to:

1. The right to be informed

2. The right of access to any of their data held by us (known as a Subject Access Request);

3. The right to rectification and ask to have inaccurate personal data changed

4. The right to erasure ('the right to be forgotten'), which is not absolute and only applies in certain circumstances

5. The right to restrict processing, which is not absolute and only applies in certain circumstances

6. The right to data portability, which only applies to information an individual has provided to the University

7. The right to 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;

8. Rights concerning automated decision-making and profiling

13.2. 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. We can extend this by two months in certain circumstances defined in the UK GDPR.

13.3. All data subjects' rights are provided free of charge.

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

Direct Marketing

13.5. The University will comply with the rules set out in the UK GDPR, the Privacy and Electronic Communications Regulations (PECR) and any laws which may amend or replace the regulations around

direct marketing. It includes, but is not limited to, contact with data subjects by post, email, text message, social media messaging, and telephone (both live and recorded calls).

13.6. Direct marketing means the communication (by any means) of any advertising or marketing material directed or addressed to individuals. “Marketing” does not need to sell anything or advertise a commercial product. It includes contact made by organisations to individuals to promote the University’s aims.

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

Complaints about Data Protection

13.8. The University is committed to ensuring that individuals can raise concerns or complaints about the handling of their personal data, and to resolving concerns or complaints promptly and transparently.

13.9. Individuals who believe their personal data has not been processed in accordance with data protection legislation and their information rights may submit a complaint through the University’s data protection complaints procedure. Complaints may be submitted in writing using the designated online complaints form or by any other contact method.

13.10. All complaints will be formally acknowledged within 30 days of receipt and will be investigated and responded to without undue delay. The University will provide the complainant with a clear explanation of the outcome of the investigation and any actions taken as a result.

13.11. If a complainant is not satisfied with the University’s response, they have the right to escalate their complaint to the Information Commissioner’s Office (ICO). Contact details for the ICO and guidance on how to escalate a complaint will form part of the University’s response.

14. Managing Risks

Data Protection Impact Assessments

14.1. The University will conduct Data Protection Impact Assessments for all new projects where processing of personal data will occur or where there is a significant change to how personal data is processed. This includes whether the processing is likely to result in a high risk to the individual or not. Any decision not to conduct a DPIA will be recorded, including the reason.

14.2. The University has a separate policy in place that governs the DPIA process.

14.3. Should the University be unable to mitigate the identified risks such that a high risk remains, it will consult with the ICO.

Dealing with Data Protection Breaches

14.4. A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, or unauthorised disclosure of, or access to, personal dataWe have procedures in place to manage the reporting lifecycle of a data breach which defines the role and responsibilities for reporting and the process that is followed.

14.5. Staff, volunteers, or contractors working for the University who experience a personal data breach must report it immediately to the Data Protection Officer.

14.6. The Data Protection Officer will consider whether the breach poses a risk to people. There will be consideration of the likelihood and severity of the risk to people's rights and freedoms following the breach. Following this assessment, the Data Protection Officer must notify the ICO if there will likely be such a risk within 72 hours of the University becoming aware of the breach. If it's unlikely, there is no requirement to make a report. There is no requirement to report every breach to the ICO.

14.7. The University will review all reports. It will keep records of all personal data breaches, even if the breach does not fulfil the criteria for reporting to the ICO. The Data Protection Officer may recommend improving practice, as breaches can provide learning opportunities.

14.8. Where a personal data breach causes a high risk, the University will (as well as reporting the breach to the ICO) inform the data subjects. It can include situations where, for example, we lose bank account details. Informing data subjects can enable them to take steps to protect themselves and exercise their rights.

Keeping Records of Our Data Processing

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

Training and Guidance

14.10. The University will provide online training, which all staff must undertake at least annually to raise awareness of their obligations and the University's responsibilities, as well as to outline the law. The training is mandatory to all employees who process personal data, irrespective of role, working location or working pattern

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

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

14.13. Failure to complete mandatory training will result in consequences as outlined in a separate HR policy on mandatory training requirements.

Schedule 1 – Definitions

The following terms appear in the University's Data Protection Policy. They have their legal meaning as set out within the UK GDPR. We explain the UK GDPR definitions below:

Automated decision-making results in decisions:

a. using personal data solely by automatic means and
b. having a significant effect on the individual concerned.

Data controller means any organisation which determines how to process personal data and the purposes for which it takes place. It does not matter if the decisions are made alone or jointly with others.

The data controller is responsible for personal data and how it is processed. The University is the data controller of the data which it processes.

Data processors include individuals or organisations that process personal data on the University's behalf and its instructions. An example is an external organisation which provides secure waste disposal for the University. This definition will include the data processors' staff (note that the staff of data processors may also be data subjects).

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

a. students
b. alumni
c. employees (and former employees) and contracted personnel
d. suppliers, professional advisers and consultants, including individuals who are the University's contractors or employees working for them
e. business contacts
f. landlords or licensees
g. volunteers
h. complainants
i. supporters
j. enquirers
k. friends and family of staff and students
l. advisers and representatives of other organisations.
m. donors and alumni
n. authors, publishers and other creators
o. persons who may be the subject of enquiry
p. third parties participating in coursework
q. health, welfare, government and social organisations
r. individuals captured by CCTV images
s. clients

t. witnesses
u. parties to legal proceedings
v. parties to transactions or dispute resolution procedures

ICO means the Information Commissioner's Office, the UK's regulatory body responsible for ensuring that the University complies with its legal data protection duties. The ICO provides guidance on implementing data protection law and can take regulatory action when a breach occurs.

Personal data is any information about a natural living person who is identified or 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. However, 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 widely defined and includes any activity that involves the data. It includes obtaining, recording, holding, storing and disposing of the data or carrying out any operation or set of processes 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 clear, moving or still images of living individuals is also a processing activity.

Special category data (as identified in the UK GDPR) include information about a person's:

a. Racial or ethnic origin;
b. Political opinions;
c. Religious or similar (e.g. philosophical) beliefs;
d. Trade union membership;
e. Health (including physical and mental health and the provision of health care services);
f. Genetic data;
g. Biometric data;
h. Sexual life and sexual orientation.

Canterbury Christ Church University

Data Protection Policy

Document information	Description of document information
Document title	Data Protection Policy
Department owner	Governance and Legal Services
Document category	**Governance -** Documents relating to the governance of the University
Document owner	University Solicitor
Document manager	Data Protection Officer Head of Data Protection
Related University policies	
Related University procedures	
Approved by	Information Governance Group
Date approved	October 2025
Date of commencement	October 2025
Review date	October 2027
Version	3.0
History of revisions of the document	1.0 approved by Senior Management Team 22 May 2018 2.0 approved by Information Governance Group, updated to take account of developments in data protection law, including exiting the European Union 3.0 approved by Information Governance Group, updated wording around non-compliance with mandatory training, DPIA requirement, data breach procedures and new complaint procedures
Web address	https://www.canterbury.ac.uk/asset-library/policy-zone/the-data-protection-policy.pdf