THE CARNEGIE TRUST
FOR THE UNIVERSITIES OF SCOTLAND

Carnegie Trust for the Universities of Scotland

DATA PROTECTION POLICY

Document status:	Approved by the Board of Trustees, 9 February 2018
Effective from:	May 2018

Carnegie Trust for the Universities of Scotland
Andrew Carnegie House
Pittencrieff Street
Dunfermline KY12 8AW
www.carnegie-trust.org
Phone: 01383 724 990
SC015600

CONTENTS

1 INTRODUCTION AND PURPOSE

1.1 The Carnegie Trust for the Universities of Scotland ("the Trust") is committed to ensuring that good information governance and data protection compliance are part of our day to day work. The Trust processes information including certain sensitive information, both of a personal and a business nature, and has a duty to protect this information and ensure it is processed lawfully and not seen or accessed by people without the authority to do so.

1.2 This policy is intended to:

- set out a framework for information governance that is fully compliant with current legislation and the requirements of the General Data Protection Regulation (May 2018); and
- minimise the opportunity for data security breaches.

1.3 The Trust is committed to providing briefing and training as necessary in relation to this policy and to raise awareness of it and to ensure compliance with it.

1.4 Any failure to comply with this policy may breach confidentiality and expose the Trust to a potential breach of trust. Non-compliance with this policy may also result in, or contribute to: theft of intellectual property, fraud and/or identity theft. Failure could also constitute a breach of the Trust's legislative, regulatory and/or contractual requirements including our statutory obligations under the relevant legislation, which would subject the Trust to a significant fine and result in a financial loss that could compromise the Trust's activities and ongoing viability.

1.5 Given the risks and the Trust's responsibilities and obligations in this area, any breach of this policy by its employees may result in disciplinary action.

2 SCOPE

2.1 This policy applies to all employees of the Trust and particularly those who process personal data on the Trust's behalf. Any contractor or agency worker/temporary worker is required to adhere to this policy as part of their contract with the Trust. It also covers the responsibilities of: the Trustees, external parties that support the work of the Trust (e.g. Assessors, Reviewers, Advisers, Referees); and any visitors to any of the Trust's premises. This policy applies to all data held by the Trust.

3 ROLES AND RESPONSIBILITIES

3.1 Whilst responsibility for implementation of this policy rests with the Secretary & Treasurer (Chief Executive) as the data controller, it is the responsibility of everyone to whom this policy applies, as noted in clause 2.1 above, to support and adhere to data protection 'good practice' at all times.

3.2 The Secretary & Treasurer has ultimate responsibility for compliance with the relevant legislation on data protection and for ensuring compliance with this policy, however, all employees are required to:

- achieve and demonstrate an adequate level of awareness of the data protection regulations, and the Trust's information security and confidentiality policies;

- familiarise themselves with, and adhere to, the key procedures, practices and guidance relating to data processing and data protection; and
- participate actively in information security and attend all related training and refresher training organised by the Trust.

3.3 The Secretary & Treasurer is responsible for the implementation of this policy, with the assistance of the Bursar as the nominated data protection lead. Any questions about data protection in general, the operation of this policy or an employee's obligations under it, should be raised in the first instance with the Bursar.

3.4 The Information Commissioner is the independent regulator charged with monitoring and enforcing UK data protection legislation whilst promoting good practice. The Trust is registered with the Information Commissioner's Office (ICO): *Registration Number: Z9592913*. Further useful information and guidance can be found on their website at www.ico.org.uk.

4 THE DATA PROTECTION PRINCIPLES

4.1 The Trust aims to fulfil its obligations under the General Data Protection Regulation and the associated legislation. This sets out six principles to be followed by all those who process data and also gives rights to those whose data are being processed. The principles require that personal data must:

a) be processed lawfully, fairly and in a transparent manner in relation to individuals;

b) be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; noting that further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

c) be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) be accurate and, where necessary, kept up to date; every reasonable step having been taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e) be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; noting that personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

f) be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

4.2 Employees must seek advice from the Bursar or Secretary & Treasurer if they are unclear about their obligations in respect of any of the six principles noted in clause 4.1.

5 THE USE OF PERSONAL DATA

5.1 The legislation is designed to ensure fairness, transparency and accountability in the processing of personal data. This means that the Trust as a data controller must comply with the six data protection principles outlined above in the processing of personal data.

5.2 **A *data controller*** is defined as any legal entity which determines the purposes and means of processing personal data. The Trust is, therefore, a *data controller* for the personal data it holds whether about employees, suppliers, students, academics, former grant holders, donors, or any other stakeholder.

5.3 ***Personal data*** is defined as any information relating to an identifiable person who can be directly or indirectly identified.

5.3.1 Personal data includes information about any one or more living individuals which the Trust holds in:

- emails;
- any other correspondence and provision of services, regardless of whether the Trust drafted it, and whether in electronic form or hard copy;
- any electronic or hard copy database or other collection of contact information;
- the form of an audio or audio-visual recording including part of recorded dictation or in a voicemail message; and
- HR and personal files and records whether in electronic form or hard copy.

5.3.2 It should be noted that one individual's opinion about another individual is personal data about both of them and therefore falls within the legislation and the terms of this policy.

5.3.3 Information about any legal person other than a living individual e.g. about a company, a partnership or a public authority, is not personal data. However, information about any individual working for that entity e.g. employees, contractors etc. is personal data.

5.3.4 ***Sensitive Personal Data*** includes information about an individual's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition, sexual life, or about the commission or alleged commission by an individual of any offence or any related proceedings or sentence. The legislation imposes additional requirements in respect of the processing of this sensitive personal data in order to ensure that it is appropriately safeguarded. Employees should therefore always take particular care when dealing with *sensitive personal data*.

5.4 ***Processing*** means holding or otherwise accessing or using personal data in any manner whatsoever including even simply reading it or telling someone about it. Employees should be aware that anything which they do with personal data in the course of their work, including obtaining it, holding it, disclosing it, using it and erasing/destroying it, is likely to amount to processing.

5.5 ***Lawful Basis for processing personal data***. The Trust will ensure that there is a recognised basis for processing each class of personal data. Appendix-A lists the main options and their identification with different groups of individuals about whom data is held by the Trust.

5.6 In most cases regarding employees, the Trust will process their data on the basis that it is necessary for the performance of the employee contract, for compliance with a legal obligation, or for the purposes of the Trust's legitimate interests. Where the Trust requires to obtain consent from the employee to process data, it will obtain that consent at the point at which the data is collected and provide specific information as to why the data is needed and the purpose(s) for which it will be used. Where consent is relied upon, employees will be made aware of their right to withdraw that consent.

5.7 **Consent and Withdrawal**. Where the Trust is processing data related to persons who are not employees, it will only process that data on a lawful basis for the instance of processing. In many cases this will necessitate obtaining consent from the individual concerned at the collection point when their data are being acquired. However, where the lawful basis arises from compliance with a legal obligation or the pursuit of legitimate (e.g. contractual) interests this should be recognised as the primary justification. All data subjects will be notified: of the intention to hold this information at the time of collection; and of their right to withdraw consent, where it has been given, or to terminate the relevant connection with the Trust that is giving rise to their data being processed. Whenever the lawful basis includes consent this will require the active agreement of the individual and will not be assumed by default.

5.8 **Privacy Notices** are the means by which individuals are notified of the Trusts requirement to hold and process their personal data. *Privacy Notices* usually include a response section in which the individual concerned indicates his or her acceptance, or otherwise, that the Trust can process their data. The Trust will ensure that its *privacy notices* comply with the relevant legislation and are shared with those whose data is being processed at the points at which the data is collected.

5.9 **Impact Assessment.** The Trust will assess the impact of changes to its operations and administrative procedures upon the protection of personal data. It will consider the appropriateness of new data processing activities and, where these differ significantly from those previously in place, will issue updated *Privacy Notices* and obtain any necessary new consents from the data subjects.

6 DATA SECURITY

6.1 Employees are responsible for ensuring that:

- any personal data they hold is kept securely and in accordance with the terms of this policy;
- personal information is not disclosed either orally, in writing, via Web pages or by any other means whether accidentally or otherwise, to any unauthorised third party;
- any information they provide to the Trust in connection with their employment or consultancy services is accurate and up to date;
- they inform the Trust of any changes to their personal information, e.g. any change of address must be notified to the Trust without delay;
- they comply with the terms of this Data Protection Policy.

6.2 Any unauthorised disclosure will usually be a disciplinary matter and may be considered gross misconduct.

6.3 Personal information should be handled securely and stored in a locked filing cabinet, drawer or safe. If it is computerised the information must be coded, encrypted or password protected both on a local hard drive and on a network drive that is regularly backed up.

6.4 The Trust will ensure that its IT systems achieve accreditation through the Government's 'Cyber Essentials' scheme, or other similar schemes as may be appropriate, to ensure the Trust is protected as far as that is possible from cyber risks and in order to demonstrate the Trust's proactive approach to security and diligence in meeting IT security standards.

6.5 Where laptops are taken off-site, employees must follow the Trust's policies relating to the security of information and the use of computers for working at home or in relation to bringing their own device to work.

7 DISCLOSURE AND SHARING OF PERSONAL INFORMATION

7.1 Employees should note that the Trust may disclose personal data it holds to third parties in certain circumstances only, including:

7.1.1 where the Trust is under a duty to disclose or share a data subject's personal data in order to comply with a legal obligation, or in order to enforce or apply any contract with the data subject or other agreements, or to protect its rights, property, or safety of its employees, customers, or other stakeholders. This includes exchanging information with other companies and organisations for the purposes of fraud protection and credit risk reduction.

7.2 Employees who are in doubt about the disclosure or sharing of personal data should seek advice from the Secretary & Treasurer in advance of any such disclosure or sharing.

7.3 The Trust will ensure that its procurement procedures require third parties who are processing data in respect of Trust employees to demonstrate their compliance with the relevant data protection legislation in force at the time.

8 TRANSFERRING PERSONAL DATA TO A COUNTRY OUTSIDE THE EEA

8.1 The Trust may transfer any personal data it holds to a country outside the European Economic Area (EEA) provided that one of the following conditions applies:

8.1.1 The country to which the personal data is transferred ensures an adequate level of protection for the data subject's rights and freedoms.

8.1.2 The data subject has given their consent.

8.1.3 The transfer is necessary for one of the reasons set out in the legislation, including the performance of a contract between the Trust and the data subject, or to protect the vital interests of the data subject.

8.1.4 The transfer is legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims.

8.1.5 The transfer is authorised by the relevant data protection authority where the Trust has ensured adequate safeguards in relation to the data subject's privacy, their fundamental rights and freedoms, and the exercise of their rights.

8.1.6 Subject to the requirements of clause 6 above, personal data the Trust holds may also be processed by employees operating outside the EEA who work for one of its suppliers. Those employees may be engaged in the fulfilment of contracts with the data subject, the processing of details or the provision of support services.

9 SUBJECT ACCESS REQUESTS

9.1 The Trust will inform data subjects, typically through a *Privacy Notice,* of the:

- types of information it keeps about her/him;
- purpose for which it is used;
- legal basis on which it is processed; and
- types of organisation that it may be passed to unless this is self-evident (for example, it is self-evident that an employee's national insurance number is given to HM Revenue & Customs).

9.2 Employees have the right to access information kept about her/him by the Trust, including personal files, sickness records, disciplinary or training records, appraisal or performance review notes, emails in which the employee is the focus of the email and documents that are about the employee.

9.3 Data subjects including employees are allowed to make a formal request for information that the Trust holds about them. Where a request for access to personal data is made the Trust will respond to the data subject access request "without undue delay" and within one month at the latest, although this may be extended by two further months where necessary, taking into account the complexity and number of requests. All such requests must be directed to the Secretary & Treasurer.

9.4 In the event that the Trust receives a request that is manifestly unfounded or excessive, it can charge a reasonable fee, taking into account the administrative costs of responding to the request, or it is entitled to refuse to act on the request. In the latter case the refusal must be justified and they must be informed of their right to complain to a supervisory authority and/or to a judicial remedy.

9.5 In the event of a disagreement regarding the accessing of an employee's personal data, the employee may pursue the matter under the grievance procedure.

9.6 Where the data subject makes a request by electronic means, the information will be provided by electronic means where possible, unless the data subject requests otherwise. The Trust will allow employees to access hard copies of their personal information under an access request.

9.7 Third parties must make access requests in writing and any employee in receipt of such a request must forward it to the Secretary & Treasurer immediately. Information will not be given via telephone enquiries. The Trust will only respond to written requests and responses must only be made by the Secretary & Treasurer.

10 BREACH OF THE POLICY

10.1 A data breach can occur due to accidental disclosure, loss through human error, flood or fire damage to premises, misuse, theft or targeted attack.

10.2 Any employee who thinks that such a breach has occurred or that they or another employee may have breached this policy must notify the Secretary & Treasurer immediately. This is very important as speedy action can be crucial in mitigating the negative effects of a breach, particularly where data security is concerned. The Trust will apply its Data Breach Notification Policy in such circumstances as required under law.

10.3 Failure to comply with this Data Protection Policy will result in disciplinary action.

11 MONITORING AND REVIEW OF THIS POLICY

11.1 The Secretary & Treasurer will be responsible for the monitoring and review of this policy and will ensure that it remains legally compliant and continues to meet the needs and aspirations of the Trust and its employees. The effectiveness of the Trust's data handling and security controls will be reviewed on a regular basis.

11.2 This policy has anticipated the requirements of the General Data Protection Regulation which comes into force in May 2018. The Trust recognises that subject to the introduction of that legislation, some refinement of this policy may be required.

Appendix-A:
Lawful bases for processing personal data

NB. Privacy Notices should include the lawful basis for processing the data collected as well as the purposes of the processing

The generally permitted options are specified in the General Data Protection Regulation, as follows:

6(1)(a) – Consent of the data subject

6(1)(b) – Processing is necessary for the performance of a contract with the data subject or to take steps to enter into a contract

6(1)(c) – Processing is necessary for compliance with a legal obligation

6(1)(d) – Processing is necessary to protect the vital interests of a data subject or another person

6(1)(e) – Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

6(1)(f) – Necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject.

We are encouraged to avoid using consent when there is a more fundamental basis available.

1.	**Students**	
1.1	Undergraduate fees grant holder	(b)
1.2	Vacation grant holders	(b)
1.3	Hardship grants holders	(b)
1.4	Former grant holders	(a)
2.	**Academics**	
2.1	Research grant holders	(b)
2.2	Former grant holders	(a)
2.3	Assessors / Panel members	(a)
3.	**Trustees**	
3.1	Current Trustees	(a) & (c)
3.2	Past Trustees	(a)
4.	**Staff**	
4.1	Current employees	(a) & (c)
4.2	Past employees	(a)
5.	**Supporters & Donors**	
5.1	Small donors (fee repayments)	(a)
5.2	Major donors	(a)
5.3	Relatives / executors of legators	(a)
5.4	General supporters (recipients of Annual Report)	(a)