

Policy and procedure

Data protection

Key messages

- The holding, using, disposing or sharing of personal identifiable data must comply with the *Data Protection Act*.
- Patients must be informed about what we use their information for by issuing them with the leaflet *What happens to information held about you* (PIN6/ PIN949)
- The personal identifiable data held by the Trust must be accurate and not excessive.
- Access to personal identifiable data is on a strict need to know basis.
- Patients have the right to access information held about them by contacting the Access to Health Records Team.

1 Scope

Trust-wide: This policy applies to all Trust employees, including:

- staff who hold honorary contracts
- contractors working on behalf of the Trust
- the Board of Governors
- non-executive directors.

2 Purpose

- to inform staff of the need to comply with the *Data Protection Act 1998* (DPA)
- to inform staff about what is expected of them and protect them as a user under the DPA
- to protect the Trust as an employer and as a user of personal information.

3 Definitions

3.1 Anonymised information

Anonymised information is information which does not identify an individual directly and which cannot reasonably be used to determine identity. Anonymisation requires the removal of name, address full post code and any other detail or combination of detail that might support identification directly or by association, for eg using someone's initials.

3.2 Database

A database is a collection of personal information that can be processed by automated means eg:

- patient records for appointments
- patient details for prescribing drugs
- patient information used for research
- staff records such as training or leavers or starters.

Databases that meet this definition could be processed either by using a custom-built software system or a MS-Access or MS-Excel program.

3.3 Data controller

A data controller is the person or organisation who either alone or jointly or in common with other persons determines the purpose for which and the manner in which any personal data is processed.

3.4 Data processor

A data processor is any person or organisation (apart from an employee of the data controller) who processes data on behalf of the data controller.

3.5 Data subject

A data subject is the individual who is the subject of the personal data.

3.6 Legitimate relationships

Legitimate relationships control who has access to a patient's health record. A team of staff or individual health professional can gain access to a patient's record if they have a legitimate relationship with the patient. Access controls to patient's records will be based on legitimate relationships and identified workgroups. Workgroups are groups of staff with identified key activities eg doctor or receptionist which determine who can access information and to what level.

3.7 Personal data

Personal data is data that relates to a living individual who can be identified either from that data or from that data and other information that is in the possession of or is likely to come in the possession of the data controller (The Trust).

Data could include items such as:

- surname
- initials
- date of birth
- address and postcode
- sex
- national insurance number
- hospital number

- forenames
- occupation
- NHS number
- ethnic group.

This is not an exhaustive list, personal data can be information that does not include any of these personal details but the individual could be identified from this information and other information in possession of the data controller by association for example medical photograph of a patient with a rare condition.

3.8 Processing

In relation to information or data, 'processing' means obtaining, recording or holding the information or data carrying out any operation or set of operations on the information or data, including:

- organisation, adaptation or alteration of the information or data
- retrieval, consultation or use of the information or data
- disclosure of the information or data by transmission, dissemination or otherwise making available
- alignment, combination, blocking, erasure or destruction of the information or data.

3.9 Pseudonymised information

Pseudonymised information is like anonymised information in that in the possession of the holder it cannot be reasonably used by the holder to identify an individual for eg a unique number used in a research project. However it differs in that the original provider of the information may retain a means of identifying individuals. This will often be achieved by attaching codes or other unique references to information so that the data will only be identifiable to those who have access to the key or index.

Pseudonymisation allows information about the same individual to be linked in a way that true anonymisation does not.

3.10 Sensitive personal data

Sensitive personal data is personal information that includes:

- religious beliefs
- political beliefs
- sexual life
- membership of a trade union
- ethnic background
- criminal convictions
- physical and mental health records.

Note: All information regarding health is considered sensitive under the DPA.

4 Introduction

This policy will apply to all personal information for living individuals recorded and held by the Trust.

The Trust holds and processes information about its employees, patients and other individuals for various purposes.

The Trust is required to comply with the *Data Protection Act 1998* when handling personal data in relation to living people.

The Trust is also governed by:

- the Human Rights Act 1998
- Section 251 and 252 of The National Health Service Act 2006
- common law on Confidentiality
- Freedom of Information Act 2000
- Environmental Information Regulations 2004
- Computer Misuse Act 1990
- NHS Code of Practice on Confidentiality
- NHS Care Records Guarantee
- NHS Code of Practice on Information Security
- Mental Capacity Act 2005
- Caldicott Guidelines
- Information Governance Toolkit
- NHS Constitution
- Access to Health Records Act.

This policy sets out how the Trust will meet these requirements.

4.1 Data protection principles

The Data Protection Act 1998 sets standards, known as the eight data protection principles, which have to be satisfied when using, holding, disclosing and/or disposing of personal information about living individuals. These standards apply to information that is held in either electronic or paper format.

The eight data protection principles are:

1. Personal data shall be processed (used) fairly and lawfully.
2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose(s).
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose(s) for which they are processed.
4. Personal data shall be accurate and kept up to date.
5. Personal data processed for any purpose(s) shall not be kept for longer than is necessary for that purpose(s).
6. Personal data shall be processed in accordance with the rights of the data subjects under this Act.

7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to personal data.
8. Personal data shall not be transferred to a country or territory outside of the European Economic Area (EEA), unless that country or territory ensures an adequate level of protection in place (see [appendix 3](#)).

4.2 Rights of the data subject

The rights of the data subject are:

- right to access personal information held about them by any organisation, known as subject access requests
- right to prevent processing
- right to request that facts recorded about them that are incorrect are either removed or corrected
- right to seek compensation if caused harm or distress
- right to ask the Information Commissioner to investigate on their behalf if they have been caused harm or distress
- rights regarding automatic processes
- rights regarding information processed for marketing purposes.

The Information Commissioner's office is responsible for ensuring compliance with the Data Protection Act 1998 and providing advice and guidance. The Trust is required to notify the purposes for which it uses personal identifiable information to the Information Commissioner.

4.3 Caldicott Guardian

Health organisations are required to appoint a Caldicott Guardian who is a senior health professional who has the seniority and authority to exercise the necessary influences on policy and strategic planning in relation to data processing and information sharing.

4.4 Caldicott principles

The Caldicott principles are concerned with the use and protection of patient identifiable information. All trusts must abide by these principles:

- justify the purpose – every proposed use or transfer of patient identifiable information within or from another organisation should be clearly defined (and reviewed if continuing)
- do not use patient identifiable information unless it is absolutely necessary
- use the minimum necessary – where the use of patient identifiable information is considered to be essential each individual item of information should be justified with the aim of reducing identification
- access to personal information should be restricted on a strict need to know basis
- everyone should be aware of their responsibilities
- every use of personal information should be lawful.

Information Governance

Directorate of Information Systems and Analysis

5 Responsibilities

5.1 Chief executive

The chief executive is legally responsible for ensuring complete and continued data notification for the Trust.

5.2 Board of Directors

The director for Information Systems and Analysis is responsible for raising issues to the Board of Directors as appropriate.

5.3 Head of Patient Services

The head of Patient Services is the nominated data protection officer for the Trust and designated Caldicott officer, responsible for renewing and maintaining adequate notification and providing advice and guidance to staff and the Caldicott Guardian.

5.4 Information governance lead

The information governance lead is responsible for:

- undertaking any duties as required by the head of Patient Services
- ensuring that the Trust complies with the Information Governance Toolkit
- providing advice and guidance to all staff.

5.5 Information Governance Team

The Information Governance Team is responsible for providing training to all Trust staff on information governance and for providing advice and guidance to staff.

5.6 Senior managers

Senior managers are responsible for:

- ensuring that all staff comply with the policies and procedures and that they attend training on a yearly basis
- implementing any necessary/ reasonable changes highlighted by audits
- ensuring that any personal data held is up to date and accurate.

5.7 Data awareness representatives

Each department's nominated data awareness representative is responsible, along with the department senior manager, for:

- ensuring that staff comply with the relevant policies and procedures
- undertaking key tasks as directed by the Information Governance Team or head of Patient Services.

5.8 All Trust staff

All Trust staff must:

- adhere to the confidentiality clause in their contracts
- attend Information Governance training on a yearly basis
- report any breaches of confidentiality
- comply with this policy.

6 Using, holding and disclosing personal information

6.1 The duty to inform

The Trust is required to inform individuals:

- why we hold their information
- for what purposes we use their information
- with whom we may share their information.

Patients must be issued with the leaflet *What happens to information held about you* (PIN6/PIN949) on a yearly basis. The issue of the leaflet must be recorded on the Alert sheet in the front of the patient's notes. This leaflet informs patients about the main uses of their information.

Supplementary information should be produced locally and provided to patients if information is used for any other purposes that are not included in this leaflet. One test for this would be to consider whether you think the patient would be surprised about how their information will be used.

The leaflet and associated posters must be displayed in patient areas.

In order to ensure that patients are informed effectively, staff should:

- check that the information leaflet has been read and understood
- inform patients when information is recorded or health records accessed
- inform patients when information will be shared with others
- check that patients are aware of the choices available to them in respect of how their information may be disclosed and used
- check that patients have no concerns or queries about how their information is disclosed and used
- answer any queries personally or direct the patient to others who can answer their questions
- respect the rights of patients.

Patients have the right to object to the use of their personal information. If this would compromise the provision of healthcare, then the risks must be explained to the patient and a compromise reached if possible.

All decisions regarding patients wishes must be recorded on the Alert sheet and as an administration code on HISS ([hospital information support system](#)). Information for staff about what the Trust does with staff personal information is contained within the [protecting and keeping confidential employee data policy](#).

6.2 Adequate, relevant and not excessive

The level of personal information held should be adequate, relevant and not excessive. The minimum amount of identifiable data should always be used, and the use of that information justified. Where possible, personal information should be anonymised, as this can be used with few constraints.

6.3 Accurate and up to date

All personal information must be accurate and up to date. This is to ensure that we provide the best possible patient care and that we run an efficient business.

Patients' details must be checked at every visit by asking open questions, for example "what is your address?". Ensure that any changes are updated as soon as possible, preferably in real time, print new labels and ID sheet and ensure old ones are destroyed.

Staff must inform their line manager of any changes to their personal details as soon as possible.

6.4 Protecting personal information

Keeping all personal information secure is vital. Opportunity puts temptation in an individual's way so all Trust staff must adhere to the security measures to protect personal information and the safe haven procedures when sharing personal information. Please refer to the [information security policy](#).

6.5 Access to personal information

All personal data must be treated as confidential and must not be disclosed to anyone who is not authorised to receive it. For further guidance on the sharing of personal information please refer to the [confidentiality of personal health information policy and procedure](#) and/or the [protecting and keeping confidential employee data policy](#).

Staff must only have access to personal data on a strict need to know basis for the purpose of the role that they are employed to do, eg

- for health care, where the employee has a legitimate relationship with a patient (this includes both health care professionals and administrators)
- for personnel issues where the employee is the line manager of another employee or is authorised to access personnel files
- where the employee is authorised to access personal data/ create records in specific circumstances eg
 - legal services in medico legal cases
 - dealing with complaints
 - clinical auditors, clinical coders, researchers
 - risk managers/ representatives
 - investigating officers
 - finance staff
 - Information Management Team.

Information Governance

Directorate of Information Systems and Analysis

Staff who are patients of the hospital must not view their own information. Staff who would like access to their health records should refer to the [subject access](#) section below.

Staff must not look up friend or family member details unless they are involved in their healthcare.

Managers are not allowed to access medical information about their staff and their staff's families.

From time to time staff will see people that they know who are themselves attending the hospital. It is important that although they will want to speak to them that they do not ask about the reason for their visit; wait for them to provide information.

Data on all electronic systems must be accessed by staff by using their own logon identifier and personal password, appropriate access controls must be in place.

6.6 Processing/ using personal information

Processing of personal data must be necessary and must comply with at least one of the conditions set out in schedule 2 of the Data Protection Act (see [appendix 1](#)). If one of the conditions in this schedule does not apply then the Trust cannot continue to process the personal data.

In addition, for the processing of sensitive personal data which includes physical and mental health information then at least one of the conditions in schedule 3 should also be met (see [appendix 2](#)).

Note:

- an individual is entitled to request that the Trust ceases or does not begin to process their personal data where it would likely to cause unwarranted substantial damage or substantial distress to them or to another
- processing private data on Trust premises using Trust equipment is prohibited
- processing personal data, whilst undertaking a course of study, is at the manager's discretion. The manager should notify the data protection officer in writing with the employee's name, reason for using the Trust equipment and the data being processed for example identifiable.

6.7 Retention and disposal of personal information

Personal information should not be retained for longer than necessary. The Department of Health sets out retention periods for a variety of documents. All information should be retained to comply with the retention and destruction schedules. For further guidance please refer to the [records preservation retention and destruction policy](#).

Information Governance

Directorate of Information Systems and Analysis

All personal/ confidential information should be destroyed securely. For further guidance please refer to the [information security policy](#) and the [waste disposal policy](#).

6.8 Education and training

Anonymised records will usually be sufficient for use in teaching purposes and education. If it is not possible to anonymise the records then explicit consent is needed from the patient.

Education portfolios should only include anonymised patient records unless explicit consent has been obtained from the patient.

External assessors/ trainers should only be given access to patient identifiable information if it is justifiable and the patient has given explicit consent.

7 Information mapping: inbound/ outbound information

Information flows should be identified for the processing and sharing of all personal information. This is to ensure that we:

- keep personal information secure
- know for what purpose we are using personal information
- comply with the safe haven procedures and the Caldicott principles.

All departments will be required to maintain an information mapping log; this must be reviewed on a yearly basis. For further guidance please contact the Information Governance Team.

8 Notification/ registration

The Trust must notify the Information Commissioner of:

- a description of the personal data being processed and the categories of the data subjects to which they relate
- a description of the purposes of processing
- a description of any recipients to whom the data controller intends or may disclose the data to
- the name or description of any countries or territories outside the European Economic Area to which the data controller transfers or intends to transfer data
- a description of the security measures taken to protect personal data.

Data must only be used for purposes declared in the Trust's notification and must not be used for other non-registered purposes.

Information Governance must be made aware of all new databases. The Trust's database registration form ([available on Connect](#)) must be completed and sent to the Information Governance Team. The purpose for the use of the data will be checked against the Trust's data protection notification so that any new processing can be added to the Trust's notification. The system will be added to the Trust's Database Register, held by Information

Governance. New systems/ processes should not be purchased or implemented until they have been approved by Information Governance.

For further guidance please refer to the [information governance policy](#).

9 Subject access

All individuals, or in certain circumstances someone acting on behalf of an individual, can request a copy of their personal data held by the Trust. An individual who makes a subject access request is entitled to:

- be told by the Trust whether any personal data is held about them, and
- be supplied with a copy of the information that forms any such personal data.

The Trust has 21 days to respond in writing to a data subject request. There are specific reasons why access to personal data may be denied including:

- where the data released may cause serious harm to the physical or mental health or condition of the patient, or any other person
- where access would disclose information relating to or provided by a third party and consent has not been obtained by that third party
- where the consultant in charge of a patient's care assesses that a patient under the age of 16 cannot understand the implication of accessing the records.

All information supplied to the individual must be in a legible format. Codes must be explained and jargon defined.

9.1 Requests from patients

Patients can approach a clinician who is currently treating them to view information held about them relating to the current treatment that they are undergoing. Alternatively, they can put in a written request to obtain access to any information held about them. All written requests for personal information should be date stamped with the date of receipt and forwarded to the access to health records officer, box 82. for further guidance please refer to the [access to health records policy](#) and [procedure](#).

9.2 Requests from staff

Employees who wish to access their personnel file should contact their manager and at a convenient time access will be allowed.

Individuals may apply for their information to be rectified, erased, blocked or destroyed if information relating to them is inaccurate or contains an expression of opinion which is based on inaccurate data. Data is inaccurate if it is incorrect or misleading as to any matter of fact.

A court may, where it considers it practicable, order the data controller (the Trust) to notify anyone who has been sent information of any rectifications, blocking, erasure or destruction of information.

10 Contract clauses

All contractors employed by the Trust will be required to comply with the Trust's data protection, confidentiality and security requirements. Contracts must include appropriate clauses to comply with information governance. For further guidance please refer to the [information governance policy](#).

11 Transfer of data outside of the EEA

Personal data cannot be transferred outside of the European Economic Area. (see [appendix 3](#)) unless the country has adequate levels of protection in place. The European Commission is responsible for deciding which countries have adequate levels of protection in place.

If identifiable information is to be shared outside of the countries in the European Economic Area please contact the data protection officer or information governance lead for further advice.

12 Automated decision making

Currently there is no automated decision making taking place, as defined under the Data Protection Act 1998, in the Trust. Any intended automated decision making must be discussed with the data protection officer before it is put in place.

13 NHS Care Records Guarantee

The NHS Care Records Guarantee sets out the 12 commitments to patients with regard to the new NHS Care Record and local patient records; this includes:

- how we share information and with whom
- patients' rights of access to information held about them
- that staff are trained in their responsibilities
- that we will adhere to the NHS Code of Practice on Confidentiality
- that we will have audit processes in place to know who has accessed patient records.

The Trust is working towards complying with all 12 commitments.

14 Training and advice

All new starters will receive the information governance code of conduct and information governance training when they join the Trust.

All Trust staff will receive an information governance update session on a yearly basis.

Communication and publicity material is available to staff as required to raise awareness and inform staff of new procedures/ current issues.

For advice regarding data protection you can contact:

- your line manager
- senior manager within your department/ directorate
- departmental data awareness representative
- data protection officer
- information governance lead
- Information Governance Team.

15 Breaches, incidents, disciplinary, compensation, complaints process

It is each member of staff's responsibility to maintain personal data in line with this policy and ensure it is secure. A breach of the Data Protection Act could result in the Trust receiving an enforcement notice, a fine or being audited by the Information Commissioner's Office. Staff who commit a deliberate or careless breach of the Act will face disciplinary proceedings which could result in the loss of employment.

Further guidance is available in the [information governance incidents and investigations policy and procedure](#).

16 Monitoring compliance with and the effectiveness of this document

Key standards to be monitored:

- the holding, using, sharing and disposing of personal identifiable information complies with the requirements of the Data Protection Act.

The standards will be monitored by the Information Governance Team by:

- undertaking information governance audits:
 - each department will be audited every 18 months
 - an audit report and action plan will be issued to each department
 - the Information Governance Steering Group (IGSG) will receive a yearly audit report on the findings of the audit program.
 - the IGSG is responsible for ensuring that any actions identified are implemented by either the Information Governance Team or department
- monitoring information risk assessments and incidents:
 - the information governance lead and IT governance lead are notified of all incidents and risk assessments relating to information governance
 - the IGSG receives a monthly report on information risk assessments
 - the information governance quarterly report includes details on the number of incidents raised
 - The IGSG is responsible for ensuring that any actions are implemented by the Information Governance Team or department.

17 References

Data Protection Act 1998
NHS Code of Confidentiality
Information Governance Toolkit

18 Associated documents

- [access to health records policy](#)
- [access to health records procedure](#)
- [confidentiality of personal health information policy and procedure](#)
- data sharing protocol procedure
- [freedom of information \(FoI\) policy and procedure](#)
- [home working policy](#)
- [information governance policy](#)
- [information governance incidents and investigations policy and procedure](#)
- [information security policy](#)
- [Internet and email use policy](#)
- [protecting and keeping confidential employee data policy](#)
- [records management policy](#)
- [records management procedure](#)
- [records preservation retention and destruction policy](#)
- [waste disposal policy](#)
- *What happens to information held about you (PIN6/ PIN949) patient information leaflet*

Equality and diversity statement

This document complies with the Cambridge University Hospitals NHS Foundation Trust service equality and diversity statement.

Disclaimer

It is **your** responsibility to check against the electronic library that this printed out copy is the most recent issue of this document.

Document management

Approval:	Information Governance Steering Group, 9 February 2010		
Owning department:	Information Governance		
Author(s):	Michelle Ellerbeck, Information Governance Lead		
File name:	Data protection p+p Version6 February 2010.doc		
Supersedes:	Data protection policy Version 5, March 2008 Data protection procedure Version 3, March 2008 (Media ID 310)		
Version number:	6	Review date:	February 2013
Local reference:		Media ID:	309

Appendix 1: Schedule 2 of the Data Protection Act 1998

At least one of the following conditions must be satisfied to legitimise processing of personal data:

1. The data Subject has given his consent to the processing.
2. The processing is necessary:
 - a) For the performance of a contract to which the data subject is a party, or
 - b) For the taking of steps at the request of the data subject with a view to entering into a contract
3. The processing is necessary for compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by contract.
4. The processing is necessary in order to protect the vital interests of the data subject.
5. The processing is necessary:
 - a) For administration of justice
 - b) For the exercise of any functions conferred on any person by or under any enactment
 - c) For the exercise of any functions of the Crown, a Minister of the Crown or government department or
 - d) For the exercise of any other function of a public nature exercised in the public interest by any person
6. The processing is necessary for the purpose of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject.
Note: The Secretary of State may by order specify particular circumstances in which this condition is, or is not, to be taken to be satisfied.

Appendix 2: Schedule 3 of the Data Protection Act 1998

At least one of the following conditions must be satisfied to legitimise processing of sensitive personal data:

1. The data subject has given his or her explicit consent to the processing of personal data.
2. The processing is necessary for the purpose of exercising or performing any right or obligation which is conferred or imposed by law on the data controller in connection with employment. Note: The Secretary of State may by order:
 - a) Exclude the application of the above paragraph in such cases as may be specified, or
 - b) Provide that, in such cases as may be specified, the condition in the above paragraph is not to be regarded as satisfied unless such further conditions as may be specified in the order are also satisfied.
3. The processing is necessary:
 - a) In order to protect the vital interests of the data subject or another person, in a case where:
 - I. Consent cannot be given by or behalf of the data subject, or
 - II. The data controller cannot reasonably be expected to obtain the consent of the data subject
 - b) In order to protect the vital interests of another person, in a case where consent by or on behalf of the data subject has been reasonably withheld.
4. The processing:
 - a) Is carried out in the course of its legitimate activities by any body or association:
 - I. Is not established or conducted for profit, and
 - II. Exists for political, philosophical, religious or trade union purposes
 - b) Is carried out with appropriate safeguards for the rights and freedoms of data subjects
 - c) Relates only to individuals who either are members of the body or association or have regular contract with it in connection with its purpose, and
 - d) Does not involve disclosure or the personal data to a third party without the consent of the data subject
5. The information contained in the personal data has been made public as a result of steps deliberately taken by the data subject.
6. The processing:
 - a) Is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings)
 - b) Is necessary for the purpose of obtaining legal advice
 - c) Is otherwise necessary for the purposes of establishing, exercising or defending legal rights
7. The processing is necessary:
 - a) For the administration of justice

Information Governance

Directorate of Information Systems and Analysis

- b) For the exercise of any functions conferred on any person by or under an enactment, or
- c) For the exercise of any functions of the Crown, a Minister of the Crown or a government department.
Note: The Secretary of State may by order:
 - a) Exclude the application of the above paragraph in such cases as may be specified, or
 - b) Provide that, in such cases as may be specified, the condition in the above paragraph is not to be disregarded as satisfied unless such further conditions as may be specified in the order are also satisfied

8. The processing is necessary for medical purposes and is undertaken by:

- a) A health professional, or
 - b) A person who in the circumstances owes a duty of confidentiality which is equivalent to that which would arise if that person were a health professional
- Note: The 'medical purposes' includes the purposes of preventative medicine, medical diagnosis, medical research, the provision of care and treatment and the management of healthcare services.

9. The processing:

- a) Is of sensitive personal data consisting of information as to racial or ethnic origin
- b) Is necessary for the purpose of identifying or keeping under review the existence or absence of equality of opportunity or treatment between persons of different racial or ethnic origins, with a view to enabling such equality to be promoted or maintained, and
- c) Is carried out with appropriate safeguards for the rights and freedoms of the data subjects.

Note: The Secretary of State may by order specify circumstances in which processing falling within a or b above is, or is not, to be taken for the purposes of sub-paragraph c to be carried out with appropriate safeguards for the rights and freedoms of data subjects.

10. The personal data are processed in circumstances specified in an order made by the Secretary of State for the purpose of this paragraph

Appendix 3: List of countries within the European Economic Area where information can be shared

If identifiable information is to be shared outside of the countries listed below, the data protection officer must be advised. The Information Commissioner will be contacted to ensure what level of protection is offered by other countries.

- Austria
- Belgium
- Cyprus
- Czech Republic
- Denmark
- Estonia
- Finland
- France
- Germany
- Greece
- Hungary
- Iceland
- Ireland
- Italy
- Latvia
- Liechtenstein
- Lithuania
- Luxembourg
- Malta
- Netherlands
- Norway
- Poland
- Portugal
- Slovakia
- Slovenia
- Spain
- Sweden

Note: This list changes on a regular basis. Date last verified as correct: