

Data Protection Policy for

Northumbria Community Trust

Contents

[1 Introduction 3](#_Toc532226079)

[1.1 Purpose 3](#_Toc532226080)

[1.2 Scope 3](#_Toc532226081)

[1.3 Definitions 3](#_Toc532226082)

[2 Policy Statement 4](#_Toc532226083)

[2.1 Data Protection Lead 4](#_Toc532226084)

[2.2 Principles of data protection 4](#_Toc532226085)

[2.3 Collecting personal data 6](#_Toc532226086)

[2.4 Privacy Notice 6](#_Toc532226087)

[2.5 Lawful bases 6](#_Toc532226088)

[2.6 Individual rights 6](#_Toc532226089)

[2.7 Data Protection Impact Assessment 7](#_Toc532226090)

[2.8 Data Sharing 7](#_Toc532226091)

[2.9 Storing of data and data security 8](#_Toc532226092)

[2.10 Video and photography 9](#_Toc532226092)

[2.11 Fact versus Opinion 9](#_Toc532226093)

[2.12 Capturing data end and destruction/deletion dates 10](#_Toc532226093)

[2.13 Data Audit and destruction of data 10](#_Toc532226095)

[2.14 Data Breaches 11](#_Toc532226094)

[2.15 Subject Access requests 11](#_Toc532226095)

[2.16 Information Commissioner’s Office 1](#_Toc532226095)2

[2.17 Training and Compliance 12](#_Toc532226095)

[3 Approval and review 13](#_Toc532226096)

[4 Revision History 13](#_Toc532226097)

[5 APPENDIX 1 – Lawful bases (from GDPR Article 6) 14](#_Toc532226098)

[6 APPENDIX 2 - Information Asset Register 15](#_Toc532226099)

[7 APPENDIX 3 – Retention schedule 1](#_Toc532226101)6

# Introduction

The protection of personal data is enshrined in UK law, but it is also a moral responsibility that the Northumbria Community Trust (NCT) takes seriously. Embedding data protection within the organisation benefits NCT, and all individuals who interact with us, by enabling uniform and consistent decision making, building a culture of awareness and responsibility, making personal data management and infrastructure more resilient; and, through transparency and accountability, instilling trust and confidence in individuals when they provide us with their data, and ensuring their rights and freedoms are upheld.

This policy should be read alongside NCT’s Privacy Notice.

For all staff and volunteers processing data for the Trust, data protection is everybody’s responsibility and requires an open and supporting each other approach to ensure the Trust is as compliant as it can be.

## Purpose

The purpose of this policy is to describe the steps that NCT are taking to comply with data protection legislation, to ensure that our compliance with the relevant legislation is clear and demonstrable.

This policy is also intended to provide us with measures for ensuring that risks to individuals through misuse of personal data are minimised, such as:

* personal data being used by unauthorised individuals through poor security or inappropriate disclosure;
* individuals being harmed by decisions made using inaccurate or insufficient data;
* individuals being uninformed by lack of transparency leading to unlawful practice;
* the invasion of privacy due to over-collection or over-retention of data.

## Scope

This policy applies to NCT.

We expect all contractors, staff and volunteers processing personal data on behalf of NCT to act in accordance with this policy (and Privacy Notice) when engaged in the business of NCT.

#### Data Controller for protection purposes

The Northumbria Community Trust, a Charitable Incorporated Organisation (registered charity number 1156630), is the data controller for data protection purposes. It is referred to in this policy as the ‘Northumbria Community Trust’ or ‘NCT’.

## Definitions

* **Personal Data** - Any information that relates to an identifiable living individual.
* **Special Categories of Personal Data** (also known as sensitive personal data) - Specific types of data that require additional care being taken when processing. The categories are: race; ethnic origin; politics; religion; trade union membership; genetics; biometrics (where used for ID purposes); health; sex life; or sexual orientation.

Other sensitive personal data such as financial information whilst not listed as a special category data by law, must be handled with additional care when processing.

* **Data processing** – Any activity relating to the collection, recording, organising, structuring, use, amendment, storage, access, retrieval, transfer, analysis, disclosure, dissemination, combination, restriction, erasure or disposal of personal data.
* **Data Protection Impact Assessment (DPIA)** - A process designed to help systematically analyse, identify and minimise the data protection risks of a project or activity.
* **Data Subject** - The individual to whom the data being processed relates.
* **Data Controller** - A body or organisation that makes decisions on how personal data is being processed. Data Controllers almost always also process data.
* **Data breach** - any occasion when personal data is: accidentally or unlawfully lost, destroyed, corrupted or disclosed; accessed or passed on without proper authorisation; or made unavailable (through being hacked or by accidental loss/destruction.
* **3rd Party Data Processors** – Other legal entities that process data on behalf of a Data Controller and under instruction from the Data Controller. Data Processors do not have the ability to make decisions about *how* the data should be processed, there should be documented instructions from the Data Controller about what the processor can and cannot do with the data (known as a Data Processing/Sharing Agreement).

# Policy Statement

Personal data that NCT collects, uses, stores, transfers, shares and disposes of must be handled in line with the following policy.

## Data Protection Lead.

NCT will appoint a Data Protection Administrator, who will:

* be contactable via the Trust office by emailing: office@northumbriacommunity.org .
* be responsible for assisting NCT to monitor internal compliance and to inform and advise on data protection obligations.
* monitor data sharing agreements, data breaches, information risk, subject access requests and compliance with data protection policies and procedures.
* be accountable to the NCT Trustees.

## Principles of data protection

Personal data is processed according to the following principles:

1. **Data is processed lawfully, fairly and in a transparent manner** in relation to the data subject, through the provision of clear and transparent privacy notices and responses to individual rights requests.
2. **Data is collected for specified, explicit and legitimate reasons** and not further processed for different reasons incompatible with these purposes. NCT will develop and maintain an Information Asset Register, that will be regularly and consistently reviewed and updated. Data that is stored and used for archiving purposes in the public interest, scientific or historical research or statistical purposes will be managed by NCT. Paper records will be stored in locked storage and electronic data on password protected data secure servers.
3. **Data is adequate, relevant and not more than is necessary** to complete the task for which it was collected and will be subject to regular review of data collection and processing needs.
4. **Data is accurate and up-to-date** and reasonable steps will be taken to ensure this through regular data quality checks.
5. **Data is not kept for longer than is necessary** to complete the task for which it was collected, by the implementation of a retention schedule (Appendix 3) and a regular data cleansing programme. Northumbria Community departments will periodically review membership lists to identify personal data for destruction. The Data Protection Administrator will lead an overarching data audit every three years to identify data for destruction. See also section 2.13.
6. **Data is kept secure**, with appropriate technical and organisational measures to protect against unauthorised or illegal processing, accidental corruption, loss or disclosure of personal data. This will include:
	* storing paper copies of personal data in locked cabinets;
	* maintaining password protection of electronic data held on computers and online storage;
	* ensuring access to paper and electronic media is restricted only to those individuals authorised to access the data.
	* ensuring that extra precautions are taken when personal data is carried in public places, to keep the risk of data breaches to an acceptable level.

To maintain appropriate data security, we will undertake regular risk assessments of our practices and provide awareness and training to all those processing personal data on behalf of NCT.

1. **Data that is transferred outside the United Kingdom** will only take place with appropriate safeguards to protect the rights of individuals.
2. **Accountability**. NCT is responsible for, and will demonstrate, compliance with the principles by:
	* Adopting and implementing this data protection policy;
	* Publish privacy notices to explain our data protection practices to those whose personal data we process
	* Put in place written contracts with 3rd party Data Processors that process personal data on our behalf;
	* Implementing periodic reviews, to update the measures we have put in place.

## Collecting personal data

Data protection legislation requires that the collection and use of personal data is fair and transparent. If we acquire any personal data related to an individual (including employees, office holders, volunteers, suppliers, supporters or other external contacts), either directly from the data subject or from a third party, we must do so in line with the above ‘Principles of Data Protection’.

If we acquire data in error (that is, data we should not have access to), by whatever means, we must inform the Data Protection Administrator who will assess whether the data should be retained and if so, arrange for it to be given to the appropriate individual.

## Privacy Notices

Individuals have the right to be informed about the collection and use of their personal data and NCT will be open and transparent about our use of personal data in line with this Policy. Our current privacy notice can be found on our website - https://www.northumbriacommunity.org

We shall maintain our privacy notice, covering our data processing activities relating to personal data. The privacy notice will be published on our website and we will provide this to individuals at the time we collect or significantly amend their personal data.

If our data processing practices change, causing a privacy notice to be updated, we will reissue the notice to the affected data subjects, by email and/or Infoodle.

## Lawful bases

Personal data must only be processed once we have identified an appropriate lawful reason to do so. There are six available lawful bases for processing (Appendix 1). No single basis is ’better’ or more important than the others, we must decide which basis is most appropriate depending on our purpose and relationship with the individual.

The Lawful basis for different areas of our data processing will be included in Information Asset Register and indicated in the relevant Privacy Notice.

## Individual rights

Data protection legislation gives individuals specific rights regarding their personal data:

1. The right to be informed – the Trust will be transparent how they use personal data
2. The right to access – the individual’s right to request a copy of the personal data held about them.
3. The right to rectification – the individual can request that data held about them be corrected
4. The right to erasure – also known as the right to be forgotten. An individual’s right to request that personal data held about them be deleted.
5. The right to restrict processing – an individual’s right to block or suppress the processing of their personal data
6. The right to data portability – an individual’s right to request that data held about them be transferred to organisations or individuals of their choosing
7. The right to object – an individual has a right to withdraw consent for how their personal data is being used. e.g. opt in and out of information sent to them
8. The right to lodge a complaint with the Information Commissioner’s Office

## Data Protection Impact Assessment

NCT has adopted the principle of privacy by design. Following the issue of this policy, all new projects, updated processes or significantly changed systems that require the use of personal data and may pose a **high risk** to data subjects, will be subject to a Data Protection Impact Assessment (DPIA). The DPIA template to be used is available via this link: https://ico.org.uk/media/about-the-ico/consultations/2258461/dpia-template-v04-post-comms-review-20180308.pdf.

The purpose of the risk assessment is to help ensure data processing risks are identified and considered, followed by putting measures in place to reduce or eliminate those identified risks.

## Data Sharing

As a data controller, we recognise that when we share personal data with third parties, we are responsible for:

* ensuring the third party complies with GDPR, and
* stating any constraints or requirements about what the third party can or cannot do with our data.

When sharing or disclosing personal data we shall ensure that:

* We consider the benefits and risks, either to individuals or the Trust, of sharing the data, along with the potential results of not sharing the data;
* We are clear about with whom we can share the data. If we are unsure, we check with the data owner, or our Data Protection Administrator.
* We do not disclose personal data about an individual to an external organisation without first checking that we have a legitimate reason to do so (see above ‘Lawful bases’ section).
* If we must transfer or share data, we do so using appropriate security measures;
* If we are sharing data outside of the UK, we take particular care to ensure that the destination country meets all the necessary requirements to protect the data.

If we are unsure whether or not we can share information, we will contact our Data Protection Administrator.

#### Data Sharing statements

We may state any constraints or requirements on the use of data shared with third parties in the following ways, depending on the level of risk:

* Through the use of disclaimer-type statements in emails or on contractor job sheets (see example below)

The following is an *example* of what is meant by ‘disclaimer type statement’ which maybe used:

The attached personal data is provided by NCT to [third\_party\_name] for the purposes of [state\_the\_purpose\_here]. To comply with General Data Protection Regulation 2016/679 and the Data Protection Act 2018, this data is only to be used for [insert\_name\_here] to contact the persons listed in the attached data file for the above stated purpose.  You must not share it with any other third party; you must store it securely and take all reasonable steps to prevent its unauthorised access, accidental deletion or corruption.  When you no longer need this data, it must be deleted and any paper copies you have made destroyed.  Should this data suffer an unauthorised disclosure (data breach), you are to notify [name and contract detail for lead data protection person].

* By the inclusion of a ‘Data Protection’ section of a contract with a third party (such as a leasing agreement)
* By a standalone ‘Data Sharing Agreement’

## Storing of data and data security

We will ensure that we use the most appropriate and secure methods available for storage and management of personal data. We will ensure that:

* In so far as we are able, all personal data in our possession is kept secure from unauthorised access;
* All physical files containing personal data to be locked in appropriately secure locked storage; Where possible archived papers will be scanned and held electronically until their destruction date.
* We are constantly vigilant of our surroundings, in particular when working outside of the Trust office, being careful not to place any personal data in a position where it can be viewed, stolen or lost;
* All devices (including smart phones, computers, tablets) used to handle personal data are password protected and we do not share passwords;
* Electronically held personal data is transmitted and backed up securely using encryption technology with appropriate information security systems in place to prevent interception. The Trust’s cloud based systems including Infoodle, Office 365 and Google Drive should be used for processing personal data off site. Electronic data security will be regularly reviewed by the Trust.
* For data security, personal email addresses should not be used for communication of personal data for Northumbria Community business. Infoodle or a Northumbria Community email address should be considered for communications including between Overseers, Trustees, the administration team and Mother House team. Those in leading roles regularly communicating personal data should request a Northumbria Community email account.
* Desks and work areas are to be kept clear of personal data when not occupied. Physical personal data must be locked away when not in use. Be aware that physical personal data could be viewed through external windows even if the office is locked.
* The Trust will adopt a segregated access approach to manage access to personal data. Access to records both electronic (including profiles in Infoodle) and paper records will be restricted to those who have a legitimate need to access those records. Where there is any doubt, then access is agreed with the Data Protection Administrator and/or Overseer responsible for Operations. When data processors end or change their roles, access to data must also be changed to reflect this. Where data processors believe they have access to data which is not required they are to report this to the Data Protection Administrator and/or Overseer responsible for Operations so this can be reviewed and appropriate action taken.
* All Northumbria Community employees must return all data belonging to the Trust on cessation of employment both paper and electronic. This includes data held on electronic media storage. All electronic devices issued by the Trust for Northumbria Community business must also be returned on cessation of employment.

## Video and photography

Photographic and video images are taken and recorded by NCT and may be shared via the Trust’s media for lawful and legitimate reasons including to pursue the mission of the Trust, to make public worship accessible online (live stream and playback), to promote Northumbria Community events and to communicate news with the Northumbria Community Companions, Novices, Postulants and Friends. See Section 2.28 for data sharing principles.

Adults in leading roles during retreats, gatherings or events can be considered as giving their consent to have their images taken and recorded as set out in the privacy notice. However, if there is any doubt especially for visitors to the Trust, then they must be consulted with and give their consent in advance of images being taken.

All other individuals attending Northumbria Community events should be consented before recognisable images are taken of them and/or shared on Northumbria Community media. All individuals have the right to object to having images taken of them and/or shared on Northumbria Community media and can request to have these removed.

Images of children should not be captured/recorded or shared on Northumbria Community media at any time without the consent of parents. Please refer to the Safeguarding Guidelines policies for Children, Youth and Vulnerable Adults for further information.

At the time of writing this policy the Trust does not nor have plans to install security CCTV on site. Should CCTV be installed, the Trust would need to register with the ICO under current guidelines (see 2.16).

## Fact versus Opinion

When using personal data, it is our policy not to write comments about any individual that are unfair, untrue or offensive and that you would not be able to defend if challenged. In general, we:

* Express facts, not opinions
* Work on the basis that anything written about an individual might be seen by that individual.

This includes emails. Although a certain amount of informality attaches to email writing, it should not be overlooked that these can provide a written record of our comments and, in the event of a Subject Access Request, they are subject to disclosure if they contain personal data.

## Capturing data end and destruction/deletion dates

Where it is will help the expediency of audits, Northumbria Community officers may record/file end and destruction dates on archived paper records. This may include any paper employment records for when officers left their post. This may help to quickly identify papers for destruction when it comes to triennial audits. Note as retention periods may change, a file closed/end date in addition to a destruction date is needed.

The Northumbria Community Operations Manager will need to record end dates for Northumbria Community members, staff and volunteers who hold certain roles. Recording end dates for roles and membership will assist with determining the deletion date of this data. Information on safeguarding roles need to be retained for long periods from when the person ended their role.

For staff and appointed volunteer roles, leaders and the Northumbria Community Operations Manager will record this information. For ad hoc volunteers and Northumbria Community members who ‘come and go’, the Northumbria Community Operations Manager will record this information as best they can. The Community Group Co-ordinator and Novitiate Co-ordinator should should review the Community Group Leaders and Novitiate Mentors roles respectively and log any end of role dates as close as possible to the end date of their role, on an annual basis. This data can be captured electronically in Infoodle.

NCT leaders need to notify the Infoodle administrator of anyone wishing to be removed from the NCT database, or those who have died, to give opportunity for their data to be end dated on Infoodle.

## Data Audit and destruction of data

The Data Protection Administrator will lead data audits.

A data audit will be conducted triennially with the purpose to identify data due for deletion or destruction by the retention periods set. This includes all paper and electronic records. Also, where found necessary to correct, archive or consolidate data. Where possible archived papers will be scanned and held electronically until their destruction date. The Trust’s Information Asset Register (See content Appendix 2) will be referred to and updated as required. All leaders will be expected to support the audit by reviewing the data they hold and identifying data for destruction.

The Trust member database on Infoodle should be reviewed annually to identify Northumbria Community members who are known to have left the Trust or died with the purpose of removing their details. Anyone wishing to be removed from the database will be sent an email asking if they would like their details removed. If they do not respond and it is confirmed they no longer wish to be part of Northumbria Community, then a second email will be sent to advise their details will be removed unless they respond within an appropriate timeframe. If they do not respond then their details will be removed. Please note some details for an individual may need to be retained for longer periods e.g. details of safeguarding roles held.

Every three years every person on the Infoodle database will be invited by email to check if their details are correct and to review their privacy preferences by logging on to ‘My Infoodle’. Those who request to be removed from Infoodle will be removed. Please note certain specific details may need to be retained for other reasons e.g. safeguarding roles held.

All paper data due for destruction will be shredded either using the Trust office cross cut shredder or for bulk shredding contracted out to an accredited confidential waste shredding company (accredited to ISO 27001). All papers identified for shredding must be securely stored until it is shredded/handed over to the confidential waste shredding company.

## Data Breaches

A personal data breach means the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes.

There will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed.

All staff and volunteers appointed to roles handling personal data for the Trust are expected to report any data breaches no matter however small to the Data Protection Administrator within 72 hours. It is recognised that low level personal data may accidentally be shared with unintended persons. These need to be reported so the appropriate steps can be taken to manage the breach in line with this policy. All staff and volunteers are expected to cooperate in full with any investigation undertaken by the data protection Lead person or ICO into an alleged breach.

***We as an organisation seek to promote a culture of openness and honesty to speak out data breach incidents no matter how small so we can respond appropriately and learn together from them to prevent more serious breaches in future.***

All data breaches are to be reported to the Data Protection Administrator. Where a breach is known to have occurred which is likely to result in a high risk to the rights and freedoms of individuals, the Data Protection Administrator will report this to the ICO within 72 hours and will co-operate with any subsequent investigation. We will contact the affected data subject(s) where it is necessary to do so.

## Subject access requests

The Data Protection Administrator with the support of the Overseer responsible for Operations shall be responsible for leading the response to these requests and will direct staff accordingly. Details for the data subject are set out in the privacy notice. These requests should be acknowledged within 72 hours and the information provided in writing as soon as possible after the request but no later than 1 calendar month. If there is a delay, then the requester must be contacted and advised of the new date.

The information requested maybe available to the data subject on Infoodle and if they can access Infoodle they can be invited to access the information from there. However, they retain right to have a written transcript sent to them if they prefer this.

## Information Commissioner’s Office

NCT will fully support the work of the Information Commissioner’s Office (ICO) when appropriate and as required by law.

The ICO maintains a register of Data Controllers, however not-for-profit organisations/charities are mostly exempt from registering. NCT is currently exempt, but if the Trust installed and operated CCTV for the purposes of crime prevention then it would be required to register. The Trust’s status in respect will be regularly reviewed in case the rules for registering change.

The ICO’s role is to uphold information rights in the public interest. The ICO can take action to change the behaviour of organisations and individuals that collect, use and keep personal information.

The ICO may use criminal prosecution, non-criminal enforcement and audit, depending on the circumstances. The ICO also has the power to serve monetary penalty notice on a data controller.

Some of the options open to the ICO where there has been a more serious breach of Data Protection Act include:

* Impose temporary or permanent ban for data processing
* Order rectification, restriction or erasure of data
* Suspend data transfer to third parties
* Issue monetary penalty notices, requiring organisations to pay up to €20m for serious breaches of EU GDPR or £17.5m of the UK DPA 2018.
* Prosecute those who commit criminal offence under the Act.

The Information Commissioner’s Office can be contacted on 0303 123 1113 or via email https://ico.org.uk/global/contact-us/email or at the Information Commissioner’s Office Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF.

## Training & Compliance

NCT will provide appropriate support and/or training to all those involved in the safe and lawful processing of personal data for the Trust.

Despite best efforts small data handling mistakes happen sometimes unnoticed. A positive and open approach to highlighting mistakes and learning from them is needed. Compliance is a team effort particularly when working under pressure of time.

We will ensure all data processors have access to this policy and the privacy notice with opportunity to discuss and clarify its content and the practical implication for data processing activities they fulfil for the Trust. Team meetings and supervision and other forums will be used for this purpose. Revised versions of the policy and privacy notice will be similarly notified to all data processors.

All NCT data processors (employees and volunteers) are expected to sign their agreement to fully comply with this policy and the Trust’s privacy notice and versions of thereafter. Particular care needs to be taken to guide volunteers in key roles not to store Northumbria Community personal data on their own electronic devices but to access it via the Trust’s secure cloud based systems such as Infoodle, Office 365 and Google Drive.

The requirement to comply Compliance with this policy and the NCT’s Privacy Notice will be reflected in all new role descriptions and employee contracts from the date this policy is first issued.

The Trustees , Overseers, Operations Manager and Data Protection Administrator will take all reasonable steps to ensure compliance to this policy.

# Approval and review

This policy will be reviewed triennially alongside the privacy notice.

|  |  |
| --- | --- |
| Approved by |  |
| Policy owner | Northumbria Community Trust  |
| Policy author |  |
| Date | March 2022 |
| Review date |  |

# Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| Version No | Revision Date | Previous revision date | Summary of Changes |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# APPENDIX 1 – Lawful bases (from GDPR Article 6)

#### Legitimate interest

The processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual’s personal data which overrides those legitimate interests.

Legitimate Interest Assessment. When can you rely on legitimate interests?

* When processing is not required by law but is of benefit to you
* When there is a limited privacy impact on the data subject
* When the data subject would reasonably expect your processing to take place

In order to use legitimate interests as your lawful basis for processing, your processing must therefore meet all of the following criteria:

* Have a specific purpose with a defined benefit
* Be necessary – if your defined benefit can be achieved without processing personal data then legitimate interests is not appropriate
* Be balanced against, and not override, the interests, rights and freedoms of data subjects

#### Contract

The processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

#### Legal obligation

The processing is necessary for you to comply with the law (not including contractual obligations).

#### Consent

The individual has given clear consent for you to process their personal data for a specific purpose.

If Consent is used it must be valid (freely given, unambiguous, actively selected, can easily be withdrawn); Both giving and withdrawing consent must be recorded.

For consent to be valid, i.e. the correct basis, it must be a choice - so if the data subject refuses to give consent, does that mean that the service can't be provided? If it is an essential service (e.g. pension, payroll etc) then the data controller cannot refuse the service, so there is effectively no choice, so consent is not valid.

#### Vital interests

The processing is necessary to protect someone’s life.

#### Public Task

The processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

For further information and assistance seek advice from [the DPO or Data Protection Lead or local registrar as appropriate].

# APPENDIX 2 - Information Asset Register

Information held on the Trust’s ‘information asset register’ will contain the following information.

The register is recorded on a separate excel spreadsheet

1. Asset number
2. Description of the data held
3. How was the data was obtained?
4. Why is the data held and what is it used for?
5. What kind of data is it? Does it contain personal or sensitive personal data?
6. Who is the owner of the data and who has access?
7. What format is the data in?
8. Where is the data stored?
9. What is the legal basis for retaining the data?
10. What is the retention period?
11. What access and security controls are in place?
12. What date was the data audited?
13. What action were there from that audit?
14. What is date of next audit?