Affordable homes.
Exceptional care.

Policy: General – Data Protection

Trust Housing Association and Wishaw & District Housing

Title of policy:	DP01 - Data Protection Policy
Date of sign off:	December 2022
Date of review:	December 2025
Lead officer:	Data Protection Officer
Scottish Social Housing Charter Outcomes & Standards:	**1, 2, 3, 7, 8, 9.**
Regulatory Standards of Governance and Financial Management:	**2, 3, 4, 5**

Data Protection Policy

Contents

1. Introduction

1.1 Trust Housing Association aims to provide homes and services of the highest standard. In doing this the Association requires to hold information that relates to tenants, service users, employees as well as applicants for housing and employment.

1.2 This document details the policy framework and the procedures and processes that Trust will follow to ensure compliance with GDPR (General Data Protection Regulations)

2. Aims and objectives

2.1 This policy aims to set out the responsibilities of the Association and its staff in processing, handling and storing information that falls within Data Protection legislation & guidance.

3. Legislative framework

3.1 The General Data Protection Regulation which defines 7 data protection principles applies to information about living, identifiable people, such as job applicants, workers, tenants and service users.

3.2 Through the data protection principles, it regulates the way information about data subjects (individuals) can be collected, handled and used.

3.3 The data protection principles state that information must be:

1. Fairly, transparently and lawfully processed
2. Processed for limited purposes
3. Minimisation of data held
4. Accurate and kept up to date
5. Not kept for longer than is necessary
6. Kept secure and confidentially

And

7. It should be demonstrable that these principles are adhered to

3.4 The GDPR also clarifies an individual's data rights, see section 8 for further details on data rights.

4. Notification

4.1 Trust Housing Association is registered as a Data Controller (Reference Z8915556)

4.2 Further information on Data Protection is available from the Information Commissioner's Office via telephone on 08456 306060 or 01625 545745 and from the website at https://ico.org.uk

5. Types of Information Held & Purpose for Holding

5.1 For the purpose of the Data Protection Policy and Procedure 'data' is classed as personal information about living, identifiable people.

5.2 The Association holds various types of information for several purposes. This information is held in accordance with the principles outlined above at point 3.3.

5.3 The Association holds information related to its landlord function, its care and support function and its function as an employer. This means that the Association holds information relating to its tenants, prospective tenants, former tenants, service users, employees, job applicants, Board and Association members.

5.4 The Association also holds information gathered via closed circuit television (CCTV) cameras at its offices and developments. This information is gathered and held in accordance with the principles outlined at point 3.3. The Association's CCTV system is operated for general security purposes only.

5.5 The Association only holds this information for the purposes of administering the above functions and will not hold information that is unnecessary or knowingly incorrect.

5.6 Information should only be gathered for an identifiable and required purpose, and this purpose should be explained to Data Subject when asking them for the data. Data gathered for one purpose should not be used for another without the express consent of the Data Subject.

5.6 There are six legal bases for processing personal data, and each category of data we process should have its legal basis identified.

- Consent - the individual has given clear consent for you to process their personal data for a specific purpose.
- 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).
- Vital Interest - 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.
- 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. (This cannot apply if you are a public authority processing data to perform your official tasks.)

6. Data Asset Registers

6.1 Trust must retain a register of all data held by the company, detailing the nature of the data and how we use it. This register enables us to be clear and transparent about what we do with data and to assess whether we are adhering to the six principles of GDPR (see section 3.3)

6.2 The Data Asset Register should include the following information:

- What category of data
- How the data was gathered
- Where the data is held
- What format the data is held in
- In what location is the data stored
- For what purpose is the data used
- What is the legal basis for holding the data?
- How long is the data retained for?
- How will the data be disposed of?
- Special Category data status
- Who do we share this data with?
- For what purpose do we share the data
- How do we share the data?
- Our relationship with the party with whom we are sharing data

6.3 The Data Asset Register should be a living document that is reviewed regularly and updated when necessary.

7. Responsibilities

7.1 All staff members are responsible for data protection and should always follow the data protection policy and procedure when dealing with data subjects' personal information. Any failure to apply the policy and procedures that causes a risk to a data subject's privacy or safety may lead to disciplinary proceedings.

7.2 The Association is registered with the Information Commissioner as a Data Controller. The Association has notified the Commissioner of the information that is held. The Data Protection Officer is responsible for the renewal of Trust's registration with the Information Commissioner.

7.3 The Association's Data Protection Officer has responsibility for co-ordinating the Data Protection Policy within Trust Housing Association. Any Data Protection enquiries to the Association should be referred to the Data Protection Officer as the identified contact person and then channelled to the appropriate member of staff.

7.4 The Data Protection Officer will consult with the Data Protection Working Group on all complex Data Protection matters that necessitate a higher degree of scrutiny.

7.5 The Data Protection Officer will provide advice and support to all departments on matters relating to compliance with the Act. The Data Protection Officer will deal with any Data Subject Access Requests and ensure that the request is

dealt with within the appropriate timescale of one calendar month. The Data Protection Officer will also monitor the Data Protection mailbox, respond to any queries and investigate any email breaches detected. The Data Protection Officer is responsible for ensuring that all work relating to Data Protection is documented, thus enabling Trust to observe the accountability principle. The Data Protection Officer is responsible for development and maintenance of all policy and procedure documentation.

7.6 Each department is responsible for adhering to the action points stated within the data protection policy and procedure. With individual responsibilities as follows:

- Chief Executive – Responsible for Office of the Chief Executive, Company Secretarial issues.
- Director of Customer Experience – Responsible for Customer Experience and Care & Support related issues
- Director of Assets and Sustainability – Responsible for Property & Development related issues
- Director of Finance and People – Responsible for People Team, Finance and Procurement
- Director of Business Development and Digital - Responsible for Service Design & Improvement and Digital & Data.
- Each Director has overall responsibility for their department or section and needs to ensure that personal data processed by their department is registered and kept up to date, the Data Controller is aware of any changes to the Data held for notification purposes and a general description of data security measures taken to protect data that they are responsible for is available

7.7 Each department or section shall appoint a Data Champion, who will have responsibility for carrying out tasks relating to the management of data within their department or section. Their responsibilities will include:

- Being the first point of contact for GDPR related questions within their department or section
- Escalating complex data protection related questions to the Data Protection Officer
- Co-ordinating with the Data Protection Officer and facilitating the gathering of personal data in the event of the receipt of a Data Subject Access Request,
- Schedule regular reviews of data being retained by the department and ensure that Data Retention schedules are adhered to and old data deleted accordingly
- Ensuring suitable Data Destruction Notices are completed for all data deleted in accordance with the Data Retention Schedule
- Ensuring that regular departmental Data Audits are carried out to review adherence to Data Protection Policy
- Reviewing and assessing daily processes for GDPR compliance, and identifying potential risks or opportunities to improve
- Referring to the Data Protection Officer any new systems or work processes that may need to be considered for a Data Privacy Impact Assessment
- Updating and reviewing the Data Asset Register to ensure it captures all data held within the department or section

8. Data Subject Rights

8.1 The General Data Protection Regulation grants all Data Subjects rights in relation to the data Trust holds about them. Those rights are:

The Right to be Informed

8.2 Individuals have the right to be informed about the collection and use of their personal data. Data subjects will be informed, in writing, of the following in all instances:

- What information the Association will be collecting relating to them
- Why this information is required
- How this information will be stored
- Who, if anyone, this information may be shared with and for what purpose?
- How long this information will be held for
- Arrangements for ensuring that information held is up to date

8.2 There is no common form for data collection. However, each department and function should ensure that, at any point at which personal information is being collected from a data subject, the subject is made aware of all the points outlined above.

8.3 Where CCTV is in operation the Association will ensure adequate and appropriate signage, providing details of why the system is in operation and who to contact regarding any enquiries.

The Right of Access

8.4 Individuals have the right to access the personal data that is held about them, the exercising of this right is commonly referred to as a Data Subject Access Request or DSAR.

8.5 Individuals can make an access request verbally, in writing or even via social media, and Trust has one month to respond to their request. Any member of staff in receipt of a request, regardless of the medium, has the responsibility to ensure the request is passed on to the Data Protection Officer for it to be acted on.

8.6 The one-month period for responding to Data Subject Access Requests begins once the Data Subject has confirmed their identity and provided detail of the specific data they require. For example, if Trust receives a request on the 3rd of September the time limit will start from the next day (4th of September). This gives the organisation until the 4th of October to comply with the request.

8.7 A guide has been developed that assists all staff in identifying when a DSAR has been made and guides them through their role in ensuring the request is acted on.

8.8 All Data Subject Access Requests will be passed to the Data Protection Officer who will review the request and determine the appropriate course of action. Only in cases where Trust has a legitimate reason should they reject any access request.

8.9 The DPO will then contact the relevant department/team and ask them to gather the requested data and pass it to them.

8.10 Those tasked with gathering the data will review all records to identify where the requested data is held. They will take copies of the records where practical and will pass all records to the DPO.

8.11 On receipt of all the requested records the DPO will draft a response letter and send it along with all supporting documents to the requester.

The Right to Rectification

8.12 Individuals have the right to have inaccurate personal data rectified or completed if it is incomplete. An individual can make a request for rectification verbally or in writing and Trust has one calendar month to oblige.

8.13 It is the responsibility of the data subject to keep Trust informed of any changes in their personal data that would affect the validity of the information held. Data Subjects should be made aware at the point of data collection that they need to inform the Association of any changes in their personal details.

8.14 Staff have a responsibility to update personal information held by the Association should they become aware of any changes. This includes data relating to both customers and individuals employed by Trust

8.15 If the data requiring rectification has been shared with any other organisation, it is Trust's responsibility to ensure that the third party is provided with the rectified data and asked to update all records accordingly.

The Right to Erasure

8.16 The GDPR introduces the right for individuals to have their personal data erased. The right to erasure is also known as 'the right to be forgotten'. Individuals can make a request for erasure verbally or in writing and Trust has one month to respond to the request.

8.17 On receipt of a request for erasure you should advise the Data Protection Officer that a request has been made and inform them what data we have been asked to delete. The DPO will consider the request to determine if there is any requirement to deny the request.

8.18 Data Subjects have the right to have their personal data erased if:

- the personal data is no longer necessary for the purpose which you originally collected or processed it for;
- you are relying on consent as your lawful basis for holding the data, and the individual withdraws their consent;
- you are relying on legitimate interests as your basis for processing, the individual objects to the processing of their data, and there is no overriding legitimate interest to continue this processing;
- you are processing the personal data for direct marketing purposes and the individual objects to that processing;
- you have processed the personal data unlawfully (i.e. in breach of the lawfulness requirement of the 1st principle);

- you must do it to comply with a legal obligation.

8.19 The right to erasure does not apply if processing is necessary for one of the following reasons:
- to exercise the right of freedom of expression and information;
- to comply with a legal obligation;
- for the performance of a task carried out in the public interest or in the exercise of official authority;
- for archiving purposes in the public interest, scientific research historical research or statistical purposes where erasure is likely to render impossible or seriously impair the achievement of that processing; or
- for the establishment, exercise or defence of legal claims.

8.20 In instances where a request to erase personal data has been assessed as legitimate and the data has been deleted, Trust has an obligation to advise any third parties with whom we have shared the data of the request. Those third parties should then be asked to delete the data in question from their own records.

The Right to Restrict Processing

8.21 Individuals have the right to request the restriction or suppression of their personal data in instances where they are not happy with the data Trust holds or the way it has been used. This is different to a Right to Erasure claim as it is a temporary measure and Trust is entitled to keep the data, it is only the use of that data that is temporarily blocked.

8.22 A request to restrict processing usually occurs as a result of another issue e.g. a Right to Rectification request, where the individual objects to their data being processed until the rectification is made.

8.23 When processing is restricted, Trust is permitted to store the personal data, but not use it in any way. An individual can make a request for restriction verbally or in writing and Trust has one calendar month to respond to the request.

8.24 On receipt of a request to restrict processing, the DPO should be advised of the request, specifying what data the request relates to and the circumstances surrounding the request (e.g. as per the previous example they may want to restrict processing until an inaccuracy in the data has been corrected.)

8.25 In order to comply with the request to restrict processing it may be necessary to:
- temporarily move the data to another processing system;
- make the data unavailable to users; or
- temporarily remove published data from a website.

8.26 Restrictions on that data should only be removed once the underlying issue has been resolved and the Data Subject has confirmed that they are happy to withdraw their request.

The Right to Data Portability

8.27 Data Subjects are entitled to ask that any personal data that they have provided to Trust, that is processed in a digital format be provided to them in a common

machine-readable digital format. This data may be requested to be passed to the Data Subject of they may ask for it to be provided to another Data Controller.

8.28 The right only applies to information an individual has provided to Trust and it does not cover data gathered about the Data Subject by Trust that's held in a digital format.

8.29 In the event of a Data Subject making a Right to Data Portability claim the Data Protection Officer should be advised. They will co-ordinate with the relevant stakeholders to ensure that the data is provided in a secure means, within one calendar month.

The Right to Object

8.30 Individuals have the right to object to the way their personal data is being processed under certain circumstances. If the objection is judged to be legitimate then we are duty bound to cease our processing of that data.

8.31 The right to object relates primarily to direct marketing activities, there are other types of processing of data that can be subject to a right to object request but those are unlikely to be relevant to the types of processing Trust does.

8.32 Direct marketing is defined as "the communication (by whatever means) of any advertising or marketing material which is directed to particular individuals". This covers all promotional materials not just commercial ones, and Trust does not need to benefit financially from the good or service being promoted. This includes promoting Trust's aims and ideals, and covers any messages which include some marketing elements, even if that is not their main purpose. However, the promotion must be specifically targeted at individuals to count as direct marketing (e.g. a newsletter made available in a common area would not count as a means of direct marketing, but one that is posted through letterboxes would).

8.33 On receipt of an objection, the DPO should be advised of who has raised the objection and to what they have objected. The DPO will review the objection to determine its merit and on acceptance of the objection will contact the relevant stakeholder to ensure the processing is halted.

8.34 The GDPR also clarifies rights in relation to automated decision making and profiling, neither of which Trust currently engages in.

8.35 All instances of Data Subjects exercising any one of these rights, must be logged, along with a record of the outcome of all work done in relation to those rights being exercised. The Data Protection Officer will maintain and update this log.

9. Secure Data Storage

9.1 Trust holds personal data in both hard copy and as electronic files, regardless of which media the data is held in, all efforts must be made to keep the data secure and access limited to those with a legitimate purpose.

9.2 All paper-based data should be stored in a locked drawer or cabinet with access based on need. Efforts should be made to convert all paper-based data to scanned electronic copies.

9.3 All electronic data should be held within the Association's secure IT system which requires a username and password to access.

9.4 Electronic data should only be transferred or saved to devices which are provided by Trust and are registered with Trust's device management software. Unregistered personal devices should only be used to remotely access data held on Trust's Office 365 tenancy. No data belonging to Trust should ever be saved locally to a personal device (PC, Tablet or Mobile Phone).

9.5 When paper-based information is not being used it should be locked away. All Terminals/PC's etc. should be locked by the user when they are away from their desk

9.6 All stored data should only be retained for a pre-determined period and disposed of as per retention schedules.

10. Secure Data Sharing

10.1 In the course of carrying out day to day operations, Trust is required to share personal data with several bodies. This will include local authorities, HMRC and our regulators. So long as there is a legitimate legal basis for the sharing of the data, we are free to do so. However, all efforts must be made to ensure that the data is shared securely and not exposed to anyone with no legal basis to view it.

10.2 Data subjects should be made aware of any organisations to which their personal information might be transferred on a routine basis. This should take place at the point of data collection.

10.3 For every organisation that we share data with, we must establish what our relationship with them is. To do this it is necessary to determine whether each party is a Data Controller or a Data Processor.

- Data Controllers own the data and determine what is to be done with it.
- Data Processors process data in a way determined by the controller as per their instruction.

10.4 Once it is established whether it is a Controller/ Controller relationship or a Controller/Processor relationship we are required to put in place a contract that establishes the terms or our relationship and agrees on the party's responsibilities. This may be a Data Sharing Agreement in the case of a Controller/Controller relationship, or a Third-Party Addendum Agreement in the case of a Controller/Processor relationship.

10.5 There are several means of sharing data, some of which are more secure than others. All efforts should be made to share data through the most secure means possible.

10.5.1 Email – is not a preferred means of sharing data as there is little control over the data once it's been shared. If this is the most secure means of sharing that's available to you, you should ensure that you take steps to protect the data. You should not have any personal data in the body of your email. Instead you should look to have the data within some other document (Word or Excel for example) and that document should be locked with a password. That password should be sent to the recipient separately from the document to reduce the risks of the data falling into the wrong hands.

10.5.2 Post – is not a preferred means of sharing data as there is no control over that data once you have sent it. If this is the most secure means of sharing data available to you then you should ensure that your letter is sent recorded delivery.

10.5.3 Social Media – Personal data should not be shared over social media or any kind of messaging app.

10.5.4 Online portal – many organisations we share data with have online portals that allow us to upload data direct on to their systems removing all risks of the data being intercepted or set to the wrong person.

10.5.5 Microsoft Teams – the move to Microsoft Teams offers us the option to share data directly with any other organisation that has a Microsoft Teams tenancy. This is a secure means of sharing and has the benefit of being able to retain control over our documents and limit what other parties do with them (e.g. you can make a document read only to stop anyone amending the file). We can continue to manage who has access to the data for as long as it exists.

11. Data Breaches

11.1 A Data Breach means a breach of security leading to 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. It also means that a breach is more than just about losing personal data.

11.2 Data Breaches can include:

- deliberate or accidental action (or inaction) by a controller or processor;
- sending personal data to an incorrect recipient;
- computing devices containing personal data being lost or stolen;
- alteration of personal data without permission; and
- loss of availability of personal data.

11.3 If you become aware that a breach may have occurred, you must report the incident to the Data Protection Officer.

11.4 The DPO shall assess the degree of threat posed and determine what action is required by law. Should the DPO require further assistance from you, you must assist them and do so with urgency as the response may be time sensitive.

12. Data Protection Impact Assessment

12.1 DPIAs are an essential part of our accountability obligations. Conducting a DPIA is a legal requirement for any type of processing that is likely to result in high risk (including certain specified types of processing). Failing to carry out a DPIA in these cases may leave us open to enforcement action, including a fine of up to €10 million or 2% annual turnover.

12.2 A DPIA also brings broader compliance benefits, as it can be an effective way to assess and demonstrate our compliance with all data protection principles and obligations. However, DPIAs are not just a compliance exercise. An effective DPIA allows us to identify and fix problems at an early stage, bringing broader benefits for both Data Subjects and Trust.

12.3 It can reassure individuals that we are protecting their interests and have reduced any negative impact on them as much as we can. In some cases, the consultation process for a DPIA gives them a chance to have some say in the way their information is used.

12.4 Conducting and publishing a DPIA can also improve transparency and make it easier for individuals to understand how and why you are using their information. In turn, this can create potential benefits for our reputation and relationships with individuals:

- Help us to build trust and engagement with the people using our services, and improve our understanding of their needs, concerns and expectations.
- Identifying a problem early on generally means a simpler and less costly solution, as well as avoiding potential reputational damage later.
- Reduce the ongoing costs of a project by minimising the amount of information we collect where possible and devising more straightforward processes for staff.

12.5 In general, consistent use of DPIAs increases the awareness of privacy and data protection issues within the Association and ensures that all relevant staff involved in designing projects think about privacy at the early stages and adopt a '**privacy by design'** approach.

12.6 A DPIA can cover a single processing operation, or a group of similar processing operations. For new technologies, we may be able to use a DPIA done by the product developer to inform our own DPIA on our implementation plans.

12.7 For new projects, DPIAs are a vital part of privacy by design. They build in data protection compliance at an early stage, when there is most scope for influencing how the proposal is developed and implemented. However, it's important to remember that DPIAs are also relevant if we are planning to make changes to an existing system. In this case we must ensure that we do the DPIA at a point when there is a realistic opportunity to influence those plans. A DPIA is not simply a rubber stamp or a technicality as part of a sign-off process. It's vital to integrate the outcomes of a DPIA back into any project plan. We should not view a DPIA as a one-off exercise to file and forget about. A DPIA is a 'living' process to help us manage and review the risks of the processing and

the measures put in place on an ongoing basis. We need to keep it under review and reassess if anything changes. If we make any significant changes to how or why you process personal data, or to the amount of data we collect, we need to show that our DPIA assesses any new risks.

12.8 An external change to the wider context of the processing should also prompt us to review our DPIA. For example, if a new security flaw is identified, new technology is made available, or a new public concern is raised over the type of processing we do or the vulnerability of a particular group of data subjects.

12.9 There is no explicit definition of 'risk' in the GDPR, but the various provisions on DPIAs make clear that this is about the risks to individuals' interests. This includes risks to privacy and data protection rights, but also effects on other fundamental rights and interests.

12.10 The focus is therefore on any potential harm to individuals. However, the risk-based approach is not just about actual damage and should also look at the possibility for more intangible harm. It includes any "significant economic or social disadvantage". The impact on society may also be a relevant risk factor. For example, it may be a significant risk if our intended processing leads to a loss of public trust. A DPIA must assess the level of risk, and whether it is 'high risk'. The GDPR is clear that assessing the level of risk involves looking at both the likelihood and the severity of the potential harm.

12.11 We must do a DPIA before we begin any type of processing which is "likely to result in a high risk". This means that although we have not yet assessed the actual level of risk, we need to screen for factors that point to the potential for a widespread or serious impact on individuals.

12.12 In particular, the GDPR says you **must** do a DPIA if you plan:

- **Systematic and extensive profiling with significant effects:** "any systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person".
- **Large scale use of sensitive data: "**processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10"
- **Public monitoring: "**a systematic monitoring of a publicly accessible area on a large scale".

12.13 The ICO has also published a list of the kind of processing operations that are likely to be high risk and **require** a DPIA.

- **New technologies:** processing involving the use of new technologies, or the novel application of existing technologies (including AI).
- **Denial of service:** Decisions about an individual's access to a product, service, opportunity or benefit which is based to any extent on automated decision-making (including profiling) or involves the processing of special category data
- **Large-scale profiling:** any profiling of individuals on a large scale.
- **Genetic data:** any processing of genetic data other than that processed by an individual GP or health professional, for the provision of health care direct to the data subject.

- **Data matching:** combining, comparing or matching personal data obtained from multiple sources.
- **Invisible processing:** processing of personal data that has not been obtained direct from the data subject in circumstances where the controller considers that compliance with Article 14 would prove impossible or involve disproportionate effort.
- **Tracking:** processing which involves tracking an individual's geolocation or behaviour, including but not limited to the online environment.
- **Targeting of children or other vulnerable individuals**: The use of the personal data of children or other vulnerable individuals for marketing purposes, profiling or other automated decision-making, or if you intend to offer online services directly to children.
- **Risk of physical harm:** Where the processing is of such a nature that a personal data breach could jeopardise the [physical] health or safety of individuals.

12.14 We should also think carefully about doing a DPIA for any other processing that is large scale, involves profiling or monitoring, decides on access to services or opportunities, or involves sensitive data or vulnerable individuals. Even if there is no specific indication of likely high risk, it is good practice to do a DPIA for any major new project involving any use of personal data.

12.15 Any major project that changes or adopts new processes or systems should be reviewed for the potential to impact on Data Protection. An assessment needs to be made to identify potential risks and the likelihood of harm to Data Subjects. For this purpose, there is a DPIA Initial Screening Form that should be completed prior to the project starting. This screening form will identify whether a full DPIA needs to be carried out.

12.16 The DPIA should be completed by the Project Manager, with assistance if necessary, from the Data Protection Officer. On completion the form should be sent to the DPO for review and comment. Only once agreement is reached should the project commence.

13. Data Retention Schedules

13.1 GDPR requires all companies dealing with personal information to ensure that they do not retain personal data for longer than necessary. This demands that all organisations that collect data have a clear schedule for the destruction of personal data which is no longer required. However, it is also good business practice to have retention schedules for all data held, not just personal data.

13.2 All departments should create and apply their own Data Retention Schedules, the timeframes of which should ensure that data is not retained longer than necessary. While the GDPR legislation does not specify recommended timeframes there should be some justification for the timeframe opted for.

13.3 GDPR also clarifies the need for it to be demonstrable that not only do we have retention schedules set up but that we are adhering to them. This requires us to document the destruction of data so we can show that it was done within the appropriate timeframe as set out in the retention schedule.

13.4 The retention schedules need to be acted on, which will require a regular exercise to identify personal data which is due to be disposed of. This exercise should be carried out on a six-monthly basis.

13.5 The recording of the destruction of data must clarify what data has been destroyed but it should not count as personal information itself. It may therefore be necessary to use anonymisation to ensure that the destruction notice is not able to identify data subjects.

13.6 The destruction of records applies to paper hard copies and digital files, so retention schedules should be applied to all files regardless of what format they are held in. Data destruction notices must be created when deleting both paper and digital files.

14. Annual Data Audits

14.1 To ensure that all Data Protection policies are being adhered to it is necessary to engage in an annual Data Audit. This exercise will give an opportunity to review how closely each department is sticking to its schedules and data protection rules.

14.2 Data Audits must be carried out on a twelve-monthly basis. On completion of the audit process the audit report should be forwarded to the Data Protection Officer who will keep them on file.

14.3 The Data Protection Officer should be advised as to when Data Audits are due to take place, this will allow the Data Protection Officer to keep track of what audits are due to be carried out and will allow them to ensure they are available to assist and answer any queries where necessary.

14.4 The individual or individuals carrying out the Data Audit should be putting themselves in the place of the Information Commissioners Office (ICO). They should d be looking to identify any problems that could come to light were the ICO to carry out their own audit of Trust's data. It is better to identifying and fix problems before the ICO get involved, thus avoiding the prospect of fines for failure to comply with GDPR rules.

14.5 The Data Audit process is required to be demonstrable, so it must be possible to show that the responsibilities of holding personal data is being taken seriously. It is therefore necessary to keep a record of Data Audits: what actions were taken, what problems were identified, what steps were taken to address the problems.

14.6 During the audit it should be considered whether the records held are being held by the most secure method possible. All reasonable efforts should be made to hold data in the most secure fashion possible. A cost/benefit analysis should be done and only in instances where the cost, (be it the effort to convert the data being highly labour intensive, or the financial costs involved would be prohibitive) would outweigh the benefit of greater data security, should that benefit be overlooked.

14.7 Daily processes should be reviewed to determine if they are being done by the most secure means available or whether there are new facilities available that would allow an added layer of security to personal data dealt with on a daily basis.

14.8 As part of the Data Audit process the Data Asset Register should be reviewed to ensure that all personal data held by the department is included in the audit process. This is also an opportunity to review the Data Asset Register to ensure it captures all personal data being held and that it reflects any changes to retention periods etc. Where new personal data is being gathered the Data Asset Register needs to be updated to reflect this change.

14.9 You should document all identified potential risks, what changes may mitigate those risks, and record any decisions made about changes to future processes. Where a decision was taken not to adopt the most secure methods, the reasons for this decision must be recorded.

14.10 On completion of your Annual Data Audit it should be submitted to the Data Protection Officer for review. Should they highlight any areas of concern or anything they feel needs to be covered by the Audit process, steps should be taken to include these in the Data Audit.

15. Training

15.1 The Association will provide all its staff with appropriate training and guidance on the General Data Protection Regulation, its importance and their responsibilities in complying with the legislation. This training is provided through the induction programme and the staff handbook.

16. Data Protection

16.1 We will comply with the provisions of the Data Protection Act 2018, which gives individuals the right to see and receive a copy of any personal information that is held about them by the Association and to have any inaccuracies corrected.

17. Anti-Bribery

17.1 The Association is committed to the highest standards of ethical conduct and integrity in all its activities and, to ensure compliance with the Bribery Act 2010, it has introduced an Anti-Bribery policy and procedures. These must be adhered to by all employees, Board Members and associated persons or organisations acting for or on behalf of Trust when undertaking any actions referred to in this policy.

18. Equality, Diversity & Inclusion

18.1 As leaders of EDI, the Association aims to promote equality and diversity and operate equal opportunities policies which inform all aspects of its business. It will ensure that it adheres to the Equality Act 2010 by being committed to equal and fair treatment for all and opposed to any form of unlawful discrimination. As

such, in considering this policy, no one will be treated differently or less favourably than others because of any of the protected characteristics as listed in the Equality Act 2010:

- disability
- gender
- gender reassignment
- pregnancy and maternity
- race, colour or nationality
- sexual orientation
- religion or belief
- marriage and civil partnership
- age

18.2 or because of any other condition or characteristic which could place someone at a disadvantage were it to be taken into account, unless this can be objectively justified in terms of the legislation.

18.3 Trust will make reasonable adjustments for disabled people where necessary and possible to do so, and will use Happy to Translate tools and procedures to help overcome a language barrier.

19. Policy Review

19.1 This Policy will be reviewed on a three-yearly basis. The purpose of the review is to assess the policy's effectiveness and adhering to current legislation and good practice, and identify any changes which may be required.

20. Documentary References

20.1 In all of the Association's official documents, where references are made to specific job titles, roles, groups or committees, such references shall be deemed to include any changes or amendments to these job titles, roles, groups or committees resulting from any restructuring or organisational changes made within the Association (or, where this policy also applies to another member of the Trust group, made within that group member) between policy reviews.