Confidentiality and Data Protection Policy

Version: 11

Last Updated: 17 June 2021

Connect housing

Contents

Appendix

A: Definitions

B: Version history

1. Scope

This Data Protection Policy sets out the organisation's commitment and approach to data protection and provides a clear frame of reference for employees to determine the organisation's standards, aims, and ideals in respect of data protection compliance. The policy's objectives are:

- To provides a clear frame of reference for employees to determine the organisation's standards, aims, and ideals in respect of data protection compliance;
- To provide information to data subjects, data processors, and the regulatory authorities about how the organisation approaches data protection compliance;

Unless otherwise stated, this document applies to all personal data processed by Connect. It applies to any natural or legal person who processes personal data for or on behalf of Connect including: employees, volunteers, board members, casual and temporary employees, directors and officers, managing agents, contractors, external organisations employed as processors and any external organisations or individuals with whom Connect shares or discloses personal data. It also applies where Connect is a joint controller or where relevant, acts as a processor for another controller.

Arrangements to manage specific data protection risks under the umbrella of this policy are contained within separate policies and procedures listed below. These documents are periodically reviewed and approved by Data Protection Working Group.

Name of Policy/Procedure	**Review Frequency**
Acceptable Use Policy	Every 3 years
Data Retention Policy	Every 3 years
Employee Privacy Statement	Annual
Customer Privacy Statement	Annual
Recruitment (Applicant) Privacy Statement	Annual
Recording by Customers Policy	Every 3 years
Information Security Policy	Every 3 years
Handling Information Rights Requests Procedure	Every 3 years
Data Protection Impact Assessment Procedure	Every 3 years
Access to Personal Information Policy and Procedure	Every 3 years

2. Personal Data

Connect processes personal information relating to customers and colleagues such as staff, contractors, temporary staff, volunteers, involved residents, Board members and suppliers. This processing supports our services to customers and enables us to manage the business.

Connect is committed to compliance with all relevant date protection legislation, including the UK General Data Protection Regulations (UK GDPR) and any subsequent regulations. Defined terms under UK GDPR are explained in Appendix A.

Connect has to comply with the seven Data Protection Principles when processing personal data. The seven principles are set out and explained in Section 3 of this policy.

Any breach of confidentiality or security breach involving personal data affects Connect's reputation as an employer and as a business. It impacts on the trust of our customers and employees who have provided us with personal details, often of a sensitive nature, about themselves and their families. It also exposes Connect to regulatory action including fines.

In the event of a deliberate breach of confidentiality or security breach individual employees can be guilty of data protection offences for example if they knowingly obtain or disclose personal data unlawfully.

The following are examples of personal data:

- Customer and staff names, addresses, dates of birth, NI numbers, etc.
- Information about medical conditions, doctors' notes, etc.
- Tenancy agreements
- Housing applications
- Job applications
- Service referral forms or electronic notes
- Housing Benefit (or other benefit) application forms
- Complaints
- Notes recorded on our housing system
- CCTV images
- Photographs of residents or colleagues
- Recorded telephone calls
- Filmed conversations

All staff are required to read and understand the Employee Privacy Statement which explains how we use and manage personal employee data within Connect.

As well as helping us to comply with data protection legislation, we believe that the guarantee of confidentiality to staff, residents and service users is fundamental to the trust customers and colleagues are able to place in the organisation. In order to

maximise this level of confidence, we will follow these guidelines for best practice in handling personal data which are based on the Data Protection Principles:

- Connect will only hold information that is relevant to the business. We will make sure that customers are made aware of the confidentiality policy at all appropriate times (e.g. at sign-up when they are given a copy of the Customer Privacy Statement, in the tenants' handbook, when making reports of anti-social behaviour, agreeing support plans, etc.). We will provide sufficient information so that the customer is aware of what will happen to the personal information that they provide. Connect's Privacy Statement will be available on the Connect website.
- Personal data will only be obtained for specific and stated purposes. Information obtained for a specific purpose will not be used for additional purposes without specific consent.
- We will make sure that the personal data collected is both relevant to the reason for collecting it and is not excessive. All personal data collected will be factual.
- We will keep only personal data which is accurate and up-to-date. We will rectify, erase or destroy inaccurate information.
- We will not keep personal data for any longer than is necessary for the purposes for which it was obtained.
- We will respect individual's rights under the UK GDPR. These are the right to be informed, the right of access, the right to rectification, the right to erasure, the right to restrict processing, the right to data portability, the right to object to processing and rights related to automated decision making & profiling.
- We will take all appropriate steps to make sure that no unauthorised people can gain access to personal data. We will do all that we can to prevent the accidental loss, damage or destruction of the personal data that we hold.
- We will normally obtain a customer's (explicit) consent before disclosing information about that customer to a "third party" that is someone outside of Connect. In the interest of providing "joined up services" we will share personal data with other parties that are involved in the care of service users such as social services, as outlined in Connect's Privacy Statement.
- There are times when a third party can request us to release information about a service user without their consent for example the Police, for the purposes of preventing and investigating crimes, anti-social behaviour and catching and prosecuting offenders or the prevention of fraud. We will carefully check such requests and only share the information that is relevant and required.

3. Data Protection Principles

Connect is committed to compliance with the following data protection principles.

3.1 Requirement that processing be lawful and fair

Personal data must be processed lawfully, fairly and transparently and must not be processed until certain conditions are met.

Specific information must be provided to the data subject at the point of capturing personal data, this should be provided in a Privacy Statement. This is the identity of the data controller (Connect Housing), the data that is captured, the purposes for which the data will be processed, whom it will be shared with, the rights of data subjects and any other information relevant in the circumstances for example any other sources we might use to supplement the data such as social services or local housing benefit.

When the customer is providing us with personal information, they must be fully aware of the consequences of giving or not giving that information. The Association must provide enough information to ensure that the customer understands what will happen to the information that they are being asked to provide.

In addition, to comply with this principle, at least one condition from the list below must be met. The Association must have at least one lawful basis for the processing of data.

- The data subject has given their consent. This is defined under Article 4(11) UK GDPR as "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her"
- It is necessary for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract (e.g. a tenancy agreement, to deliver support services to a customer).
- It is necessary for compliance with a legal obligation to which the controller is subject (e.g., it is necessary by law for the Association to hold information about the immigration status of its employees as the Association must have confirmation that the employee is legally entitled to work in this country.);
- It is necessary to protect the vital (life or death) interests of the data subject or of another person.
- It is necessary for the performance of a task carried out in the public interest (e.g planned maintenance and repairs)
- It is necessary for the purposes of the legitimate interests of the Data Controller or by a third party. (e.g to comply with any legal obligation or when the customer may be thought to be a danger to the public, the Association would be in a position to inform the relevant authorities).

Where data is processed on the basis of legitimate interest it is very important to establish and be clear about the legitimacy of the interests pursued by the data controller or the third party. The processing will be unwarranted where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data (in particular where the data subject is a child).

Example: Processing is not 'fair' if:

- The data subject was misled or deceived
- The subject is not provided with information about:
    - The identity of the data controller (i.e. the Association)
    - The purposes of processing (i.e. if we say what we want the information for and the consequences of giving it)
- If the data is considered to be a special category of personal data at least one condition from the list below must also be met.
    - Data subject has given their explicit consent
    - The data has been made public by the data subject
    - It is necessary due to employment law (A condition in schedule 1, Part 1 DPA 18 must be met for this to apply)
    - It is necessary to comply with legal obligations that the data controller is subject to
    - It is necessary to protect vital (life or death) interests of the data subject where consent cannot be given
    - It is necessary for reasons of public health and for medical purpose by a person who owes the same duty of confidentiality as a health professional (A condition in schedule 1, Part 1 DPA 18 must be met for this to apply)
    - It is necessary due to legal proceedings for obtaining legal advice or defending legal rights
    - It is equality data to ensure that equal rights are maintained whilst ensuring safeguards for the rights and freedoms of customers.
    - It is necessary for other reasons of substantial public interest (A condition in Schedule 1, Part 2 DPA 18 must be met for this to apply)

3.2 Requirement that purposes of processing be specified, explicit and legitimate

The purposes of personal data collection must be legitimate, explicitly documented, and specified. Personal data must not be handled in any manner that is incompatible with the stated legitimate purposes.

Example: When data is processed, it must be for the purpose originally stated. If a customer has been told, 'I need this information for your complaint', staff cannot use it as evidence in an anti-social behaviour case.

3.3 Requirement that personal data be adequate, relevant and limited to what is necessary

Organisations must only collect the volume of personal data that is adequate and relevant to the purpose for which the data is collected. The personal data collection must be limited to the extent that is necessary to fulfil the stated legitimate purpose.

Example: When speaking with a customer, staff must always ensure that the information recorded is factual. Conversations that include information which is not relevant to the purpose (such as gossip or hearsay) must not be recorded.

3.4 Requirement that personal data be accurate and kept up to date

Personal data must be accurate and kept up to date.

Example: Client data validation exercise on ethnic origin and household composition. If a customer viewed their file and found the data recorded was not accurate, they have the right to ask us to change it.

3.5 Requirement that personal data be kept for no longer than is necessary

Personal data processed for any purpose must not be kept longer than is necessary for that purpose in accordance with Connect's Data Retention Policy.

3.6 Requirement that personal data be processed in a secure manner

Data collectors and processors must ensure the personally identifiable data they hold is collected, processed and stored in a manner that guarantees appropriate security of the data.

3.7 The controller shall be responsible for, and be able to demonstrate, compliance with all of the above principles (accountability)

In practice, it means all data controllers must have appropriate technical and organisational measures to be compliant with UK GDPR

4. Information Classification Scheme

Personal data may be used and communicated in a variety of formats, e.g. paper based, electronic, verbal, visual, etc. It is essential that appropriate levels of security are used for all methods of communication. The levels of security from lowest to highest may be summarised as:

Level 1: Public
This is information that has been approved by Connect and is available in the public domain, e.g. information on the Connect website, customer information leaflets, annual reports, etc. If these documents contain information about individuals, it has been anonymised and cannot be used to identify someone.

Handling, disposal and distribution of this type of data are unrestricted.

Level 2: Personal Data
All of this information reveals personally identifiable data. Much of the information at this level may be accessed by all members of Connect's staff team and it is all classed as confidential. A security breach of this information would have a high impact but a limited scope.

Handling and distribution of this type of data is restricted to staff, employees and contractors.

The disposal rules for this type of data are that it must only be held for as long as it is necessary for the purposes for which it was obtained and relevant to the business of Connect. Paper records must be destroyed by shredding when they are no longer relevant. Computer records should be purged periodically in accordance with Connect's Data Retention Policy.

Level 3: Limited Audience
This information is available only to staff on a "need-to-know" basis. For example, only a limited number of staff need to have access to the full criminal record of a specific customer. However, there may be aspects of that criminal record that may be relevant and should be shared with the wider staff team. A security breach of this information could have a very high impact.

Handling of this type of data is restricted to line managers or staff members agreed upon by all parties.

The disposal rules for this type of data are that it must only be held for as long as it is necessary for the purposes for which it was obtained and relevant to the business of Connect. Paper records must be destroyed by shredding when they are no longer relevant. Computer records should be purged periodically in accordance with Connect's Data Retention Policy.

Level 4: Highly Confidential

This information is available only to specific named staff and only when strictly relevant. A security breach of this type of information could be business-critical with an extremely high impact on the business. Or it could be life-critical for named individual(s).

The handling rules for this type of data are that it must be restricted to specified individuals only such as directors.

The disposal rules for this type of data are that it must only be held for as long as it is necessary for the purposes for which it was obtained and relevant to the business of Connect. Paper records must be destroyed by shredding when they are no longer relevant. Computer records should be purged periodically in accordance with the Data Retention Policy.

The Senior Manager Business Assurance is responsible for establishing the information classification scheme and ensuring compliance with it. The security level of specific information will be used to inform decisions about access to view, amend or delete, set standards for data sharing, and ability to print.

The security of paper-based information is ensured by following office security procedures for example using locked filing cabinets and desks and secure premises. Confidential information will not be taken off-site without the specific permission of a member of Management Group for Level 2 and Leadership Team for Levels 3 and 4. The security of verbal communication (e.g. customer interviews, phone conversations, staff discussions, etc.) and visual images (e.g. CCTV footage) is directed by stated good practice.

The security and integrity of information held electronically on the association's network is governed by Connect's 'Acceptable Use' policy. Improper use of the association's network means that the security, functionality and integrity of all information stored by Connect is at risk and any breaches will be viewed with great seriousness. The 'Acceptable Use' policy covers information accessed while on-site, in main offices and at supported housing projects and off-site for example at staff homes, customers' homes, etc. Access to electronic information off site should be via Connect Housing laptops or by remote access SSL/VPN.

USB and other memory devices, CDs, DVDs and e-mail attachments must not be used to either store or transfer information. If electronic information needs to be saved or transferred to systems outside the Connect network, specific Leadership Team level permission must be requested and the information must be encrypted.

5. Data Protection Impact Assessments

A Data Protection Impact Assessment (DPIA) is a process to help identify and minimise the data protection risks of a project. It is a legal requirement to undertake a DPIA under certain circumstances where special category data is processed, data is monitored on a systematic scale, where data is used for profiling with significant effects, or where any

planned processing is likely to have the potential for a widespread or serious impact on individuals.

Where required, the DPIA should be undertaken by the project lead before the processing commences. Upon completion, it should be returned to the Senior Manager Business Assurance for review. A record of all DPIAs will be reported quarterly to the Data Protection Working Group and logged by the Business Assurance Team.

If the DPIA identifies a high risk which cannot be mitigated against, the Senior Manager Business Assurance will consult with the ICO before starting processing.

Further guidance on completion of DPIAs is contained within the separate Data Protection Impact Assessment Procedures.

6. Responsibilities

All Connect colleagues including permanent and temporary staff, contractors, volunteers, involved residents and Board Members have a responsibility to make sure that they keep confidentiality as set out in this policy.

6.1 Chief Executive

The Chief Executive is the accountable officer responsible for the management of the organisation and ensuring appropriate mechanisms are in place to support service delivery and continuity. Protecting data and thus maintaining confidentiality is pivotal to the organisation being able to operate.

6.2 Directors

Each Director, in their respective areas of responsibility must ensure that all staff members are aware of this policy, other relevant policies and procedures, and their responsibilities concerning the processing of personal data. Each Director must ensure this policy is adhered to.

The Director of Finance and Resources has overall responsibility for the management of Data Protection within Connect and chairs the Data Protection Working Group on a quarterly basis.

6.3 Management and Supervisory Staff

Managers and supervisory staff are responsible for ensuring that all data processing operations under their control or sphere of responsibility or commissioned by them are undertaken in compliance with this policy and other relevant data protection policies. They are responsible for ensuring that anyone processing data is sufficiently aware of this policy and how it applies to their job

role and sufficiently trained to carry out their duties in compliance with this policy.

For managers, it is also important to ensure that operational procedures reflect the correct application of data protection requirements within teams that collect or process personal data; and periodic and ongoing monitoring checks are undertaken by managers to ensure compliance with data protection.

6.4 Partner & Third-Party Responsibilities

Any Third Party or organisation that is commissioned to process data or receives data from Connect, or is able to access any personal data which is within the custody of Connect must enter into a legally enforceable agreement with the Connect, the nature of which will be determined by the level of involvement with the data that is held/shared/accessed. Any such agreement must be approved by the Senior Manager Business Assurance.

All Connect colleagues including permanent and temporary staff, contractors, volunteers and Board members will sign a confidentiality undertaking before they are allowed to access any type of confidential information.

Colleagues will not gain (or attempt to gain) access to information that they are not authorised to have.

At the end of employment, all confidential information (in any format) acquired by colleagues in the course of their employment will be returned to Connect.

All information originated, amended or processed in any way for or from the Board or committees is to be regarded as confidential. The Chief Executive is responsible for ensuring that Board members adhere to this policy.

Any gross default or gross misconduct in connection with the Confidentiality and Data Protection Policy or Acceptable Use Policy is a disciplinary offence and may result in employment being summarily terminated.

Information Security personnel shall ensure appropriate technical and ICT organisational measures are in place to safeguard personal data from unauthorised access, amendment or deletion.

7. Telling Customers about the Confidentiality and Data Protection Policy

Customers must always be supplied with a copy of the customer Privacy Statement at sign-up for any type of tenancy. A copy of the Customer Privacy Statement and the Confidentiality and Data Protection Policy is made publically available on Connect's website.

If a customer already knows at sign up that there is someone (a relative, friend or support worker) who they would want us to discuss information with regarding their tenancy, the customer must be asked to sign a consent form advising us who they are granting consent to share information with and in what situations

The customer is advised through the Customer Privacy Statement which agencies we will normally share information with and under what circumstances, e.g.

- Local Authorities in connection with Universal Credit/Housing Benefit
- Utility Companies in connection with unpaid utility bills
- The Police in connection with crime prevention and prosecution of offenders
- Other situations outlined in our information sharing protocols

In addition, we also have a number of Data Processors that we share information with; these are organisations that are instructed to complete work on our behalf, such as boiler repair companies, builders etc. Usually the information that is processed will be limited to names and addresses for the purposes of completing repairs, maintaining buildings etc.

During the tenancy, a tenant must be advised about the Customer Privacy Statement when they:

- Request a third party to communicate with us on their behalf
- Complete an anti-social behaviour complaint form
- Complete a Universal Credit/Housing Benefit form
- Sign onto a support scheme

Customers who sign up for one of our supported housing or floating support schemes must be asked to read and sign an Information Disclosure Form. The form explains the security around personal details and the reasons for sharing this information.

All customers (whether general needs, supported housing or floating support schemes) must be given a copy of the Customer Privacy Statement at sign-up. This document is also available on Connect's website.

8. Data Processors

The organisation reserves the right to contract out data processing activities or operations involving the processing of personal data in the interests of business efficiency and effectiveness. No third-party data processors may be appointed who are unable to provide satisfactory assurances that they will handle personal data in accordance with the Data Protection Legislation.

People wishing to appoint a data processor will ensure that appropriate due diligence is undertaken on the proposed data processor in the field of information governance and

data protection compliance prior to their appointment. The Business Assurance Team shall provide advice and guidance in respect of this.

A written agreement shall be implemented between the organisation and the data processor which at least meets the requirements of the Data Protection Legislation. The Senior Manager Business Assurance shall ensure that a register of such agreements /arrangements is maintained. The data processing agreement will specify what is to happen to personal data upon termination of the data processing agreement.

No employee is permitted to commission or appoint a third party to process data on behalf of the organisation without adhering to this policy. The Senior Manager Business Assurance shall maintain operational instructions on the steps to take to appoint a data processor.

8.1 The organisation as a data processor

Where the organisation acts as a data processor it shall ensure it retains records of processing activities which record at least the information required under Article 30(2) of the GDPR for each controller it acts on behalf of. The organisation shall ensure that it has an appropriate agreement in place with each data controller and shall ensure that its employees, volunteers, staff and contractors, receive appropriate training to enable them to ensure compliance with the instructions and contractual terms of each data controller.

The Senior Manager Business Assurance shall implement measures to ensure that this policy is complied with.

9. Personal Data Breaches

A personal data breach is a security incident that has affected the confidentiality, integrity or availability of personal data. UK GDPR makes it clear that when a security incident has taken place, we MUST quickly decide whether a personal breach has occurred and if so, promptly take steps to address it, including telling the Information Commissioner's Office (ICO) if required.

Data Protection regulations place a duty on all organisations to report certain types of personal data breaches to the ICO, within 72 hours of Connect becoming aware of the breach (where feasible).

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data.

Therefore staff must inform their line manager as soon as they are aware that a breach of confidentiality has occurred or when confidential information has been lost.

The line manager must make the Business Assurance Team aware at the earliest opportunity.

The Chief Executive is responsible for ensuring relevant people are engaged in the investigation process including appointing a Lead Investigator.

The Lead Investigator is responsible for investigating the security incident or personal data breach and taking the appropriate action including liaising with other staff as necessary;

The Senior Manager Business Assurance is responsible for ensuring all employees are trained in their responsibilities concerning security incidents and data breaches and determining whether a security incident is a personal data breach and liaising as necessary with the ICO.

If a confidential document is found, it must be placed in an envelope marked 'confidential' and arrangements must be made to give it to a relevant line manager as soon as reasonably possible.

Where a personal breach has occurred, we need to establish the likelihood and severity of the resulting risk to a person's rights and freedoms. Examples of data breaches include malware attacks, sending information to an incorrect recipient, and system hacking as a result of poor password management. Where the likelihood is high then the ICO must be informed.

Any decision to report to the ICO must be agreed with Leadership Team. All decisions (to report or not to report) should be documented on the data breach register with supporting reasons. If Connect requires longer than 72 hours after becoming aware of the breach/loss, reasons for the delay MUST be provided to the ICO.

Connect's managers and directors are responsible for taking immediate action once they are aware that a breach of confidentiality or a data breach. This includes, but is not limited to:

- Completion of a data breach form which must be passed to the Business Assurance Team as soon as possible.
- An investigation of the nature and causes of the breach/loss
- The Business Assurance Team will report to the Leadership Team where any serious breaches have taken place with recommendations for required action, including reporting to the ICO.
- A decision about who else must be informed of the breach/loss. This will be done in conjunction with the Business Assurance Team and Leadership Team where the ICO may need to be informed
- Informing the customer of the breach/loss if appropriate, and providing the individuals with any necessary advice
- Considering the potential adverse consequences (risks) to the individual(s) if the personal data breach/loss is not addressed in an appropriate and timely manner, and what remedial action may be necessary.

- Consider if it is necessary to notify third parties ie Police.
- Whether the breach/loss merits disciplinary action – intentional or repeated accidental breaches of confidentiality by any member of staff may be subject to disciplinary action.

A full report of the incident must be passed to the Senior Manager Business Assurance. A log of breaches and any remedial action required to prevent similar breaches in the future is maintained by the Business Assurance Team.

The Data Protection Working Group has oversight of all data breaches and makes recommendations for improvement as necessary.

In the event of a breach, a service user has a right to complain to the Information Commissioner, in addition to using Connect's own complaints procedure.

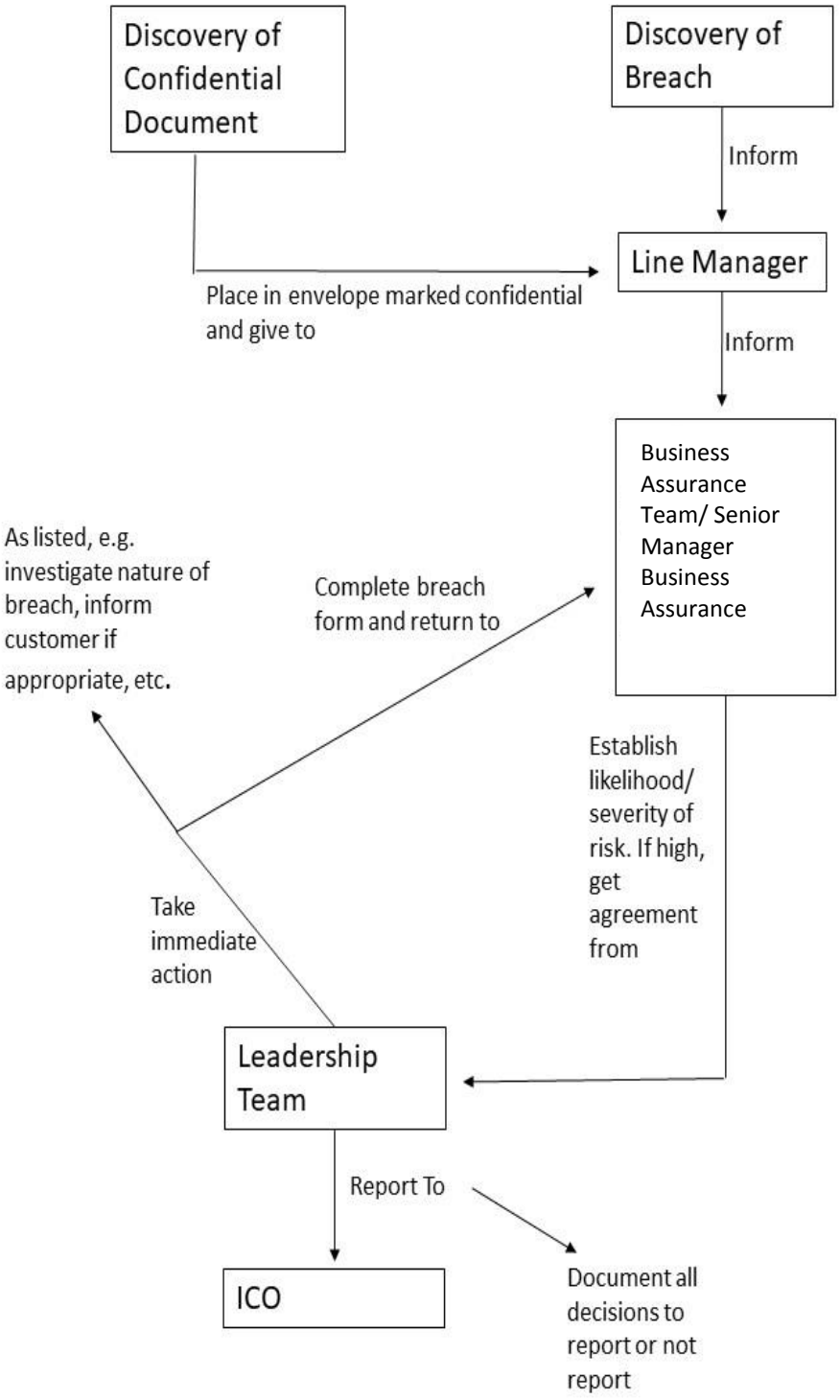
A service user can claim compensation if any harm has been caused by a breach that results in:

- The loss of personal data
- Unauthorised destruction of personal data
- Inaccurate personal data
- Unauthorised disclosure of personal data

The courts may also award compensation for any distress that has been suffered as a result of a breach.

REMEMBER - Failing to notify the ICO of a breach when required to do so can result in a significant fine of up to £8.7 million or 2% of organisation's annual turnover.

9.1 Data reporting flow chart



10. Disposal of Information

Confidential information must be held only for as long as it is necessary for the purposes for which it was obtained and relevant to the business of Connect.

Any confidential paper records must be destroyed by shredding when they are no longer relevant. Computer records should be purged periodically in accordance with Connect's Data Retention Policy.

The period for holding information is not prescriptive. Reviews of former tenants' files must take place every 5 years. Summarise relevant information and dispose of unwanted paperwork securely.

Recommended data retention periods are set out in the Connect Housing Data Retention Policy.

11. Disclosure of Information to Third Parties

Connect regularly receives requests for information about our service users from external agencies and other third parties. Colleagues must exercise great care and caution in the disclosure of any information relating to a service user to a third party. The more sensitive the personal data, the more serious are the consequences if there is an unauthorised disclosure.

In most cases, Connect will not disclose any personal data without first obtaining written consent from the customer. If you are asked to disclose confidential personal data without first obtaining consent, you must consider the following guidelines.

Questions to ask in order to clarify if disclosure is appropriate

- Do we have a statutory obligation that means we are required by law to disclose certain information, e.g. to the Police or Universal Credit/Housing Benefit? If yes, disclose the information. Note that there is only a statutory obligation to provide information to the police where they have a court order. For any other transfer, you should refer to the Senior Manager Business Assurance. The Senior Manager Business Assurance must be satisfied that the transfer can be made in a manner compliant with data protection legislation, otherwise they should refuse the transfer to the police.
- Is it necessary to disclose relevant information to other organisations for the purposes of the prevention and the investigation of crimes (including anti-social behaviour) and for the apprehending and prosecution of offenders? If yes, disclose the information.
- Was the customer made aware when the information was obtained that it could be passed, under certain circumstances, to other agencies? Does the request fall inside the possible circumstances and uses of which the service user was notified when the information was obtained? If yes, disclose the information. If no, contact the service user for their consent explaining the circumstances of the enquiry.
- Are there concerns about risks to safety, particularly in areas of child and adult protection? If yes, disclose the information.

- Do we have an information sharing protocol or data processing agreement in place with the third party (e.g. police, support agency, etc.)? If yes and the information requested is covered by the protocol, then disclose the information.
- Do we have written permission from the customer on record? Is the customer physically with the third party and can they confirm that they are willing for the disclosure to the third party? If yes, disclose the information.
- Is the information already available to the public? If yes, disclose the information.

Information required before a disclosure can be made

- Establish that there is a genuine need to know. Check that the request clearly outlines the information needed and the reason that it is required.
- Verify the identity of the person making the request. Take a name, address and general switchboard telephone number so that the person can be called back at their work place – do not take a direct number as this will not confirm who the person works for. If they are in Connect offices, look at their I.D. and photocopy or record details from it.
- Whenever possible, obtain the request in writing and respond in writing.

When decisions are made to disclose information without consent, the fact of the disclosure and the reasons for it, must be recorded. If a decision to disclose information relating to a colleague is made, Human Resources must record the reason for disclosure in the relevant personnel file. If a decision to disclose information relating to a customer, it must be recorded on the customer database. Care must be taken that all recorded information is factual.

12. Data Subject Rights

Data Subjects are people whose personal data is stored or being processed. Connect has an obligation under the UK General Data Protection Regulation (UK GDPR) to protect this information.

Guidance for employees on how to action a Data Subject Rights Request in line with the General Data Protection Regulation is contained within the separate Handling Information Rights Requests Procedure.

All employees are responsible for ensuring that any Data Subject Rights requests are passed to the Business Assurance Team without delay. Any complaints made in relation to the scope of this policy should be reported to the Senior Manager Business Assurance for resolution. The Senior Manager Business Assurance is responsible for dealing with all Data Subject Rights Requests in line with this policy.

Connect Housing has the contact details of its Senior Manager Business Assurance published on its website. We have clear guidelines on the website that enables data subjects to lodge a subject rights request or a complaint.

Connect Housing clearly provides data subject(s) with its Privacy Statement by publishing it on its website.

Under the GDPR, data subjects have the right:

- To be provided with any and all information held about them, within one month and free of charge – see Data Subject Access Request (DSAR) Checklist.
- To delete or erase their personal data, where appropriate, within one month and free of charge – see Data Subject Deletion/Erasure Request Checklist.
- To have incorrect or incomplete information rectified, within one month and free of charge – The information in question will be rectified and the data subject informed in writing, when the request has been completed.
- To have any or all processing of their personal data restricted – Processing will be suspended until the processing in question has been resolved or the restriction has been lifted.
- To object to processing, including marketing, automated decisions and profiling – When such a request is received from a data subject Connect Housing will, without undue delay, comply and stop such processing.
- To have their information made available in a readable format and portable to another organisation. Connect Housing will respond so such requests by providing the requested information in a Comma Separated Variable (CSV) file format. Where it is not technically feasible to transfer the data to another organisation, Connect Housing will treat the request for data portability as it would a data subject access request.
- To lodge a complaint with the supervisory authority (ICO). All complaints will be investigated following Connect Housing's Complaints Procedure.
- To a fair judicial remedy if their complaint is not resolved or handled to a satisfactory standard – Any such complaints will be handled by the Senior Manager Business Assurance, taking legal advice, including liaison with the supervisory authority (ICO) or the applicable appointed court of law.
- To claim compensation from the controller, processor or the supervisory authority for infringement of their rights. Any such complaints will be handled by the Senior Manager Business Assurance, taking legal advice, including liaison with the supervisory authority or the applicable appointed court of law.

Data subjects can complain about:

- how their personal data have been processed;
- how their request for access to data has been handled;
- how their complaint has been handled;

Any complaints will be handled by the Business Assurance Team in compliance with Connect Housing's Complaints Procedure.

13. Use of CCTV

All offices and support schemes that use CCTV cameras must make sure that all electronic records made are stored, viewed and deleted in accordance with the ICO CCTV code of practice. Responsibility to ensure that this good practice is followed and that all staff are clear about the procedures rests with the relevant Service Manager and Senior Manager Wellbeing and Support Services for supported housing schemes and with the Senior Manager Information Services for the main office bases.

Appendix:

A: Definitions

Commissioner: The Information Commissioner ("ICO") is the UK's independent authority set up to uphold information rights in the public interest, it promotes openness by public bodies and data privacy for individuals. The ICO reports directly to Parliament. The most relevant part of the Commissioner's duty is to ensure that data controllers are working in accordance with Data Protection regulations.

Data Protection Helpline: 0303 123 1113
https://ico.org.uk/

Data Controller: This refers to the Registered Social Landlord as the person/people who determines the way in which the information will be processed. All Data Controllers must pay a fee to the ICO unless they are exempt.

Data Processor: This refers to any person or body that processes information on behalf of the Data Controller but who does not work for them. This includes contractors, researchers, mailing houses etc

Data Subject: This means the individual that the information is about or relates to. (A person who is deceased is not a data subject.)

Examples of 'data subjects':

- Existing tenants (regardless of tenancy type)
- Ex-tenants
- Leaseholders
- Licensees
- Applicants
- Past, present and future survey respondents
- Clients receiving support
- Colleagues
- Board Members

Explicit Consent: This is also known as express or direct consent. This means that the data subject has unambiguously expressed their agreement to action we propose to take with their information. Sufficient and clear information must be given to the customer so that they understand what will happen to their personal data and can then decide if they want to give consent.

Personal Data: This is information that identifies a living person or which can be used with other information to identify a living person.

Examples of Personal Data:

- Age
- Name and contact details
- Marital Status
- Housing history
- Household type
- Economic Status
- Benefits Information
- Attitudinal Data

Processing: "Processing" means any activity involving personal data including obtaining, holding, using, disclosing and deleting it.

Nothing has to be actually done with personal information when it is "processed". UK GDPR is implicated by merely holding the information.

Special Categories of Personal Data: Some data is more personal and intimate than other data. UK GDPR recognises this and has additional requirements for handling this information appropriately.

Special categories of personal data includes:

- Racial or ethnic group of the data subject
- Political opinion of the data subject
- Religious or philosophical beliefs
- Whether the customer is a member of a trade union
- Physical or mental health
- Sexual life
- Genetic and Biometric information such as fingerprints and retina scans

Note: Personal data relating to criminal convictions and offences is not considered as special categories of data under UK GDPR, however there are similar safeguards that apply as processing can only be carried out under the control of the official authority.

B: Version History

Version	Date	Summary of Changes
11	June 2021	Reviewed by external consultant. Removal of procedures with the intention of creating a suite of standalone policies/procedures to operate alongside the Confidentiality and Data Protection Policy and Procedure. This policy is due for review in 3 years time.
10	May 2018	Updated to include data subject rights procedures and changes due to GDPR.
9	February 2018	Updated processes for confidentiality undertakings at Appendix 3
8	November 2017	Jonathan Barr of Data Protection People reviewed and amended policy in preparedness for the GDPR/DP Bill 2018
7	October 2015	Changed Corporate Services Officer to Corporate Secretary. Amended procedure of Customer Access to Personal Data: 10.2, 10.3 and 10.4
6	February 2015	Amended by DP consultant to include IA recommendations from audit eg practical guidance on responsibilities of operational staff ie additional clauses 4.1.1, 4.1.2 and 4.7 and Appendix 10. Change of title Customer Services Manager to Corporate Services Manager
5	November 2013	Reviewed by external consultant. Title amended. Some general re-wording. 2.4 and 2.6 added in Policy. Additional bullet 2. 2.1 verbal communication.
4	November 2012	Changed Customer Services Manager to Customer Services Manager and Senior Housing Advisor to Senior Housing Liaison Officer
3	September 2011	Change to 9.7 Requests from Utility Companies in line with recent clarification of legal guidelines
2	November 2009	New Confidentiality Policy Undertaking to increase clarity about Security and link to Acceptable User policy. Updated procedures to reflect improved practice. Approved by MT in Jan 2010
1	April 2006	Approved by Management Team April 2006