Data Protection Policy and Procedure

Policy Number: 02-01

Version Number: 06

Document Owner: Ozcan Yaren – Quality Manager

Signed off by: Lindy Shufflebotham – Director of HR and Quality

Date last reviewed:	**15/07/2024**	
Due date for next review:	**31/01/2026**	
Policy consultation with:	**SMT**	
Legal Requirements:	**The Data Protection Act 2018 (UK GDPR)** **Health and Social Care Act 2008**	
CQC:	**(Regulated Activities) Regulations 2014: Regulation 10 Dignity and Respect**	
Other:	**Outward is registered as a Data Controller with the Information Commissioners Office (Registration Number: Z1216891)**	
Related Policies:	**Subject Access Requests Procedure**	**Newlon Group IT Policy**
	Security Incident Handling Policy	**Code of Conduct**
	Newlon Group CCTV and Surveillance Policy	
Scope: This policy and procedure will be applied irrespective of the race, gender, marital status, disability, sexuality, religious belief or age of the employee concerned. This policy covers all employees including sessional staff and volunteers. **All Outward employees, paid or unpaid, are expected to comply fully with this policy and related procedures. Data protection is referred to in the Staff Code of Conduct and breaching this policy could lead to action under Outward's Disciplinary Procedure.** **Staff must pay particular attention to Data Protection Procedures from Page 5.**		
Policy Equality Impact Assessed		

Version number	Amendments	Reviewed by	Date
06	Data Breach reporting form has been added.	Ozcan Yaren	15/07/2024

This information can be made available in alternative formats, such as easy read or large print. Please contact 0208 980 7101 or email info@outward.org.uk.

1. Policy Statement

Outward is committed to maintaining high standards of security and confidentiality in relation to all information about people we support, staff and others. Outward will only collect, collate, process and keep information which is required for a specific purpose and which is not irrelevant and excessive for that purpose. The objectives of this policy are:

- To coordinate the information security and data handling procedures at Outward.
- To promote confidence in the organisation's information security and data handling procedures.
- To provide assurances for third parties when dealing with Outward.
- To comply with the data protection laws.
- To provide a benchmark for employees on information security, confidentiality and data protection issues.

The Data Protection Policy is also supported by our open communication policy on information handling, which means that we inform people we support and representatives of third parties with whom we work of how we use information and the purposes for which information is processed.

Outward will allow individuals access to their personal files. In the case of staff, this will be their personal file on SelectHR. In the case of people we support, this will be their care and support records, both paper and on iplanit. In the case of tenants, this will their tenancy management files on Orchard.

2. Purpose

The UK General Data Protection Regulation (GDPR) regulates how organisations handle personal information relating to living individuals. The UK General Data Protection Regulation (UK GDPR) came into effect on January 31, 2020. This date corresponds with the United Kingdom's exit from the European Union, and it marked the beginning of the UK's independent data protection framework. The UK GDPR is based on the European Union's General Data Protection Regulation (EU GDPR) but has been adapted to suit the UK's legal and regulatory environment following Brexit.

The regulation is designed to safeguard the use of personal data by laying down detailed conditions for how information should be collected, processed and stored. It also gives individuals a number of legal rights in relation to their personal information.

Our data protection obligations start from the moment we collect personal information and continue until such time as the information is returned, deleted or destroyed. People's rights in respect of their personal data apply for the same period.

Outward is fully committed to meetings its obligations under the Data Protection Act 2018, the UK General Data Protection Regulation (UK GDPR) 2016/679 and associated legislation ('the Data Protection Laws'). This policy sets out Outward's aims in relation to how we will collect and use information about people with whom we work in order to carry out business and services.

This policy applies to all personal data and special categories of personal data held in Outward's electronic networks, paper files and any other relevant filing system, including photographs, images and CCTV. (For guidance on photographs and images, see Appendix 01 (AP1); and on the use of CCTV, see Appendix 02 (AP2).) The policy may also include information on current, past and prospective people we support, tenants, employees and Board members, suppliers, contractors and members of the public.

This policy applies to all Outward employees and Board members, paid or unpaid ('the Outward Staff'). All Outward staff are expected to comply fully with this policy and its related procedures. Data protection is referred to in the organisation's Code of Conduct and breaching this policy could lead to action under Outward's disciplinary procedure. A breach of the data protection laws can lead to Outward incurring a penalty fine of up to £17 million, legal action against Outward and damage to Outward's reputation.

All contractors and service providers who access and use Outward's personal data to provide services on our behalf are expected to comply with the data protection laws. Guidance on ensuing that third parties meet our data protection requirements is set out in Outward's data protection procedures.

The purpose of the data protection laws is to regulate how organisations handle personal data. The data protection laws are designed to safeguard the use of personal data by setting

out specific conditions for how information should be collected, processed, stored and destroyed.

It also gives data subjects a number of legal rights in relation to their personal data.

3. Definitions

Data Controller: a person who determines the purpose and ways in which personal data is processed. Outward is a data controller in relation to personal data it collects, uses and stores relating to the people we support, tenants and other data subjects.

Data Processor: a person who processes data on behalf of the data controller, other than an employee. For example, Outward's maintenance contractors have access to tenants' contact details in order that they can arrange repairs, so they are data processors.

Data Subject: a living, identifiable individual about whom we hold personal data. Outward's data subjects include the people we support, tenants, staff and any other individual whose personal data we collect and use.

Personal Data: any information relating to a data subject that can be used to identify that person, whether alone or in combination with other information we have or can reasonably access. This includes pseudonymised personal data but excludes anonymised data or data that has had the identity of an individual permanently removed. It also includes expressions of opinion about an individual.

Personal Data Breach: any act or omission that compromises the security, confidentiality, integrity or availability of personal data or the physical, technical, administrative or organisational safeguards that we or our third party service providers put in place. The loss, or unauthorised access, disclosure or acquisition of personal data is a personal data breach.

Special Categories of Personal Data: any personal data about a living individual which relates to their racial or ethnic origin; political opinions; religious beliefs or other beliefs of a similar nature; physical or mental health or condition, sexual life or sexual orientation; and whether they are a member of a trade union.

We also treat the following types of information as special category personal data: the commission or alleged commission by individuals of any offence, and the proceedings for any offence committed or alleged to have been committed by them, the disposal of proceedings or the sentence of any court.

Relevant Filing System: a set of information relating to individuals and structured in a way that allows ready access to information about a particular individual. This may be electronic and will include information held in Dynamics 365, SharePoint, Orchard, SelectHR, Sona, Emails, IPlanit or Care Planning and Recording solutions, and network drives. Most paper records will also fall within this definition.

4. Principles of Data Protection

The data protection laws regulate the use of personal data through principles, which all organisations are legally obliged to comply with. Outward expects all staff to apply these principles when handling the personal data of our people we support, tenants, suppliers and colleagues.

The principles require that personal data:

- Shall be processed lawfully, fairly and in a transparent manner in relation to individuals.
- Shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
- Shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- Shall be accurate and where necessary kept up-to-date.
- Shall not be kept longer than is necessary for the purpose or purposes.
- Shall have appropriate technical and organisational measures taken against unauthorised or lawful processing, accidental loss or destruction.

For further information in relation to applying these principles, see the Data Protection Principles and the UK GDPR **Appendix 04 (AP4)** and Outward Privacy Notice **Appendix 06 (AP6)**

5. Data Subject's Rights

The Data Protection Laws provide Data Subjects with rights in relation to the information that Outward holds about them on some computer and paper records. Not all of the rights apply all of the time. These rights include:

- **Right of subject access:** Anybody has the right to make a written or verbal request for details of Personal Data about them held by Outward, and in most cases, a copy of that Personal Data.
- **Right to rectification:** Individuals have a right to have inaccurate information about them rectified.
- **Right to erasure ('right to be forgotten'):** Individuals have a right to have Personal Data about them erased by Outward in certain circumstances specified by the Data Protection Act 2018.
- **Right to restriction of processing:** Individuals have the right to require Outward to restrict its use of their Personal Data.
- **Right to object:** Individuals have the right to object to processing of Personal Data which they consider to be unlawful.

- **Right to data portability:** Individuals have a right to obtain and reuse their Personal Data for their own purposes.

This right allows individuals to move, copy or transfer Personal Data easily from one IT environment to another in a way which is safe and secure.
Where Outward is using Personal Data as a result of the Data Subject providing their consent for it to do so, the Data Subject is entitled to withdraw that consent at any time. If consent is withdrawn, this will not affect the lawfulness of Outward's use of the Personal Data prior to the withdrawal of consent.
Information about subject access requests is contained in Subject Access Requests Procedure. Outward staff must immediately forward any data subject requests received to Dataprotection@outward.org.uk. As the Data Protection Lead, the Director of HR and Quality responsible for the management of this.

6. Sharing Information within the Group

Outward shares personal data within the Newlon Housing Trust Group in order to deliver and improve services across the Group. Outward will only share personal data with the third parties where it has a lawful basis for doing so.

7. Data Protection Procedure

7.1 Storage Information

Confidential information about staff or people we support must be securely locked away and never left unattended. This includes personal information which must be held in secured locked cabinets with appropriate key holding procedures in place.
Where information is held in supported housing or the homes in which our people we support live with others, information should always be held, as a minimum, in a locked cabinet or a locked cupboard in the office. People we support and visitors entering staff offices must be escorted by staff at all times. No personal information should be left open to breach – e.g. on desks, notice boards or in unsecure post trays. For guidance on Outward's clear desk policy, see Appendix 03 (AP3).

Confidential information stored on the server must be saved within the relevant folder for the service, with appropriate settings on folders based on 'need to access'. Access is provided according to job role, and application for access is signed off by managers via IT request forms.

No personal information regarding people we support, staff or other interested parties is to be held on memory sticks (USB) or any other unprotected storage devices. When not at their computers, staff must lock their screens and never leave confidential information displayed on screen when not at their desks.

No personal information about people we support, staff or sensitive information about the organisation should be held on laptops, phones or other IT devices. All information must be stored within the Citrix system.

Any records that are confidential but have to be readily available in an emergency should be stored in an identified locked space, ensuring that a minimum amount of information is contained in the document.

Confidential data in paper form, including that relating to people we support and staff, should not be taken away from offices or services unless absolutely necessary (e.g. if attending a meeting and information is required urgently) and then only be management. Wherever possible, other ways to transport information should be used (e.g. via secure email to meeting attendees or by using a laptop/tablet and accessing via Citrix).

On the rare occasions when information needs to be taken out of the office, all reasonable care must be taken to protect that information from loss or breach.
When taking staff or people we support data away from offices, in each case permission must be sought from the area manager and due care and attention must be taken to protect the information. Data must never be left unattended – e.g. in a car. A log must be kept in each service which should be signed and countersigned when any such personal data has been taken and returned.

7.2 Disclosure of information

It is the responsibility of every person within Outward to ensure that information of a confidential nature is only disclosed within the organisation or to a third party if they are satisfied that the disclosure satisfies the following principles.

Disclosure to people outside of Outward will usually only be made with the informed consent of the person about whom the information refers. Where information is disclosed, the file will record the disclosure.

Explicit permission is not required where:

- There is a legal obligation to provide the information to an outside agency.
- There is good reason to suspect that a criminal offence has been committed.

- The individual or another person or persons is regarded to be at serious risk.

Information will only be disclosed with or without express consent in the following circumstances:

- It is to be used for the reason for which it is supplied.
- It will only be used in accordance with Outward policies and procedures for it to carry out its business and staffing functions.
- It is to be used by people within the organisation in order that they can effectively carry out their duties for which they are employed by Outward.

At times, judgements will need to be made for situations that do not fall neatly within the scope of this policy and related procedures. All such judgements must be treated with care and attention. A judgement to withhold information from the subject of a file or to disclose it to others must be authorised by a senior manager within Outward.

7.3 Correspondence and telephone calls

Any confidential information sent to Outward must be marked as such and only opened by the named individual. Telephone calls about people we support or employees should be taken in private where possible and, if not possible, then the person we support/employee should not be identified during the call.

Staff must never open person we support's mail unless the person we support is present and asks staff to do this for them. Support plans should clearly state if the person requires support for managing correspondence and the form this support should take.

7.4 Information held about people we support

People we support must feel safe and trust staff when discussing their support needs. The duty to maintain confidentiality of people we support information is therefore fundamental to providing services for people with support needs. Outward recognises that the information held about its people we support is often very sensitive and private and will ensure that this information is treated with the utmost dignity and respect at all times.

It is vital that staff have a consistent approach to confidentiality and understand their responsibilities in maintaining confidentiality. Staff will be inducted to these principles by way of training and through the core induction process.

People we support will be given information on what they can expect from Outward in relation to their personal information. This will be part of people we support handbooks and will include the principles that:

- Outward staff will seek only relevant information from other agencies.
- All information may be shared with other members or Outward staff on a need-to-know basis for safe working practices and for the health and safety of the people we support or to ensure support is provided appropriately.
- Information will not be divulged to external agencies without person we support informed consent unless the non-disclosure poses a serious threat of harm to the person we support themselves or to others.

7.5 Relevant information

In order to assess what level of support a new person we support may require and to determine if Outward can provide a service, information will be sought for each new referral. Staff should ensure that referral agencies are aware of the purpose of requiring such information and should also be specific about the type and level of information required. This would usually include medical history, social services care assessment, current needs and risk assessments. As a minimum, Outward would expect a current needs and risk assessment to establish if a support service could be offered.

In terms of who needs to know information held about a person we support, it would be safe to say anyone who is involved in assessing and/or providing the support to the person we support. This may include external agencies as well as other members of Outward staff.

7.6 Maintaining confidentiality

While providing support to a user, staff are expected to maintain a professional approach in all communications and ensure they do not discuss private information about other people we support. Staff are expected to abide by Outward's Code of Conduct, which they all read and sign a declaration to abide by.

Outward will endeavour to make every reasonable effort to ensure that individuals are able to understand the information contained in their files. This may require signage, translations or careful explanation. Where an outsider is brought in to facilitate this, e.g. signer, advocate or translator, the person who is the subject of the file will need to give his or her consent.

Any person who is not an Outward employee who may be brought in as a translator, signer or advocate will be made aware of this policy and must agree to abide by its terms.

People we support should be assured that information held about them is held securely and will be destroyed appropriately, e.g. shredded after they leave the organisation in line with regulations regarding retention and disposal timescales. Electronic records will be disposed of in the same timeframes as paper records.

It is important that all file notes, case reports and correspondence with third parties is accurate, professional and non-judgemental, so that people we support may be reassured of the organisation's commitment to its values. People we support should be made aware of their rights under data protection law which allow them access to their personal information and the right to amend any inaccuracies.

Where a third party agency request personal information about a person we support, other than for assessment or support purposes, they should be asked to put this request in writing. This will be discussed with the person we support and they should be asked for permission in writing before any information is shared.

Meetings regarding people we support should take place in private settings whereby other people we support cannot overhear what is being discussed.

7.7 Information held about staff

Throughout employment and for six years following the termination of employment, Outward will need to keep information for purposes connected with the individual's employment (e.g. payroll and reference purposes). Information we keep about staff may include:

- Information from the recruitment process, such as application forms, references and interview notes
- Details about the terms of employment, such as contracts of employment
- Payroll, tax and NI information
- Information relating to the individual's performance, like appraisals
- Details of the grade and job that staff do
- Absence records, including those related to health
- Details of any disciplinary proceedings
- Training records
- Contact names and addresses

This list is not exhaustive.

The information held on staff will be for management and administrative use only, but from time to time we may need to disclose information to relevant third parties (e.g. where we are legally obliged to do so or where we are asked by an employee for a reference, we will only state the facts in this matter). We may also transfer to another group or organisation, solely for the purposes connected with an employee's career or the management of the organisation's business (e.g. if there is a transfer under the Transfer of Undertaking (Protection of Employment) Regulations (TUPE).

Outward might hold the following information about a member of staff for which disclosure to any person will be made only when strictly necessary for the purposes set out below:

- The health of a member of staff, for the purposes of compliance with our health and safety and occupational health obligations.
- For the purposes of personnel management and administration, e.g. to consider how an employee's health affects their ability to do their job and, if the employee is disabled, whether they require any reasonable adjustment to be made to assist them at work.
- The administration of insurance, pension, sick pay and any other related benefits in force from time to time.
- In connection with unspent convictions to enable us to assess and employee's suitability for employment.

Information about staff will be held on SelectHR or otherwise in secure and lockable storage and will be accessible only to limited, relevant people.

7.8 Reporting missing information, or data protection breach

Where it becomes apparent that personal information may have been misplaced, lost or where there has been a known breach of information (someone has accessed/read information for which they do not have a right to do so) a data breach report form Data Breach Report Form (outward.org.uk) must be completed and processes followed as a 'serious' incident.

The Data Protection Lead and the relevant head of service must be informed as soon as possible.

Following on from an internal investigation to ascertain if a breach is likely to have occurred, the Executive Team will be informed of the outcome and, where necessary, appropriate

reporting will be undertaken to agencies such as Information Commissioner's Office (ICO), CQC and/or the local authority.

All incidents regarding data protection will be logged and held by the Data Protection Lead in Outward.

7.9 Staff training and induction

Staff responsibilities in relation to data protection and adherence to this policy will be covered during each employee's induction. All staff must read this policy as part of their induction and recorded and signed on the induction checklist.

All staff will be required to undertake data protection training within their six month probation period and followed by mandatory refresher training every 3 years. Monitoring of this will be carried out through the monthly KPI/PI Dashboard and Training report as a key performance indicator.

Staff can obtain information and guides to data protection from the Information Commissioner's website at www.ico.org.uk.

8. Performance Monitoring

- Training KPI's monitored monthly
- Annual quality audits of services, including reviews of data protection systems
- Service spot checks, including data protection reviews

9. Implementation of the policy

- Core induction
- Localised induction
- Intranet
- Managers e-Bulletin

10. Appendices

- AP1 Use of photographs/images
- AP2 Use of CCTV
- AP3 Clear desks
- AP4 Data Principles and GDPR
- AP5 Photo/Video Consent Form

- AP6 Privacy Notice
- AP7 Privacy Impact Assessment Template

11. General Data Protection Regulations Statement

Outward is committed to compliance with the General Data Protection Regulations and the Data Protection Act 2018. It requires all staff and partners to respect confidentiality and data subjects' rights in line with its policies and procedures.

To ensure compliance with the Regulations staff must ensure that any personal information produced or processed as part of these procedures is appropriately filed on SharePoint, Sona, Iplanit, the Outward server or other agreed Password-controlled filing system(s) with role-based access control.

Whilst processing paper documents, including those from third parties, these documents must be stored in secure lockable cabinets. Records will be kept for as long as they are needed to meet the operational needs of Outward, together with legal and regulatory requirements. Where there is a deviation from this principle, the reasons for this must be recorded.

A detailed breakdown of retention and deletion of records can be found in Outward's Record Management and Retention Policy.

When disposing of documents containing personal data this should be done via confidential waste.

Please refer to Outward's Data Protection Policy and Procedure for more information.