Data Protection Policy and Procedure

Policy Number: 02-01

Version Number: 08

Document Owner: Quality

Signed off by: Ozcan Yaren – Data Protection Lead

Date last reviewed:	19/11/2025	
Due date for next review:	19/11/2028	
Policy consultation with:	Executive Team	
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
	Records Management and Retention	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.		
Policy Equality Impact Assessed		

Version number	Amendments	Reviewed by	Date
06	Data Breach reporting form has been added.	Ozcan Yaren	15/07/2024
07	Merged with Security Incident policy. AI usage procedure has been added.	Ozcan Yaren	25/03/2025
08	Expanded glossary, added Lawfulness of processing and Data Protection by Design and Default, added information on Automated Individual Decision Making.	Elizabeth Leslie	19/11/2025

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 HR portal. In the case of people we support, this will be their care and support records, both paper and on digital care and support portals. In the case of tenants, this will their tenancy management files on housing tenancy systems.

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 31st 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, volunteers, 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 £17.5 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 ensuring 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

Cookies: A cookie is a small text file that is downloaded onto 'terminal equipment' (e.g. a computer or smartphone) when the user accesses a website. It allows the website to recognise that user's device and store some information about the user's preferences or past actions

Criminal Offence Data: personal data relating to criminal convictions and offences or related security measures

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 tenant's contact details in order to arrange repairs, so therefore 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, genetic or biometric data, 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 structured set of information relating to individuals, organised in a way that allows easy access to details about a specific person. This may be in electronic format, including data held in Dynamics 365, SharePoint, Orchard, the HR and recruitment system, the rostering system, emails, the care planning and recording system, and network drives. Most paper records will also fall under this definition.

Lawful Basis of Processing

UK GDPR Article 6 sets out the lawful basis for processing. Processing personal data under a lawful basis must be necessary and it must serve a specific, proportionate purpose. If the same goal can reasonably be achieved through less intrusive means or with less data, the lawful basis does not apply. Individuals have the right to be informed about the lawful basis for processing, this is outlined within the privacy notice. The chosen lawful basis also determines which data subject rights apply.

In order to process personal data at least one of the below must apply:

- **Consent**: clear consent to process personal data for a specific purpose has been obtained.
- **Contract**: processing is necessary for a contract Outward has with the individual, or because the individual has asked Outward to take specific steps before entering into a contract for example a referral.
- **Legal obligation:** processing is necessary for Outward to comply with the law.
- **Vital interests:** processing is necessary to protect someone's life.
- **Public Task:** processing is necessary for Outward to perform a task in the public interest or for Outward's official functions, and the task or function has a clear basis in law.
- **Legitimate interests**: processing is necessary for Outward's 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.

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.

4.1 Consent

If relying on consent as a basis for processing, there are criteria that need to be met, including:

- **Consent must be informed**: at a minimum, the individual providing consent must be told the identity of the data controller and the purposes of the processing.
- **Affirmative action**: the individual must take some form of affirmative action to provide consent; inactivity, silence or pre-ticked boxes cannot be relied on.
- **Distinguishable**: the request for consent must be clearly distinguishable from other matters and cannot be bundled up with other agreements and declarations.
- **Freely given**: the supply of the service cannot be contingent on consent being provided, where the consent is not necessary for such service.
- **Right to withdraw consent**: individuals must be informed of their right to withdraw their consent at any time.
- **Granular**: the request for consent must cover all processing activities being carried out for the same purposes. When the processing has multiple purposes, separate consent should be given for each of them.

These criteria apply not only to a new consent obtained but also any existing consent already in place. If any existing consent does not meet these requirements, it must be renewed or another legal basis sought in order to comply with GDPR.

When someone is not able to provide consent, we need to involve their family members/legal guardians/advocates in the decision.

4.2 Special Categories of Personal Data

Outward collects and processes special categories of personal data for a variety of reasons. In most cases this information has been obtained directly from the data subject. However, all Outward staff should check that there is a lawful basis for collecting or using special categories of personal data and should not do so without adequate justification and in the majority of cases not without the explicit consent of the person concerned.

Outward staff must immediately forward any data subject requests received to Dataprotection@outward.org.uk. Outward's Data Protection Lead is responsible for the management of this.

For further information in relation to applying these principles, see the Outward Privacy Notice **Appendix 04 (AP4)**

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 computer and paper records. Not all of the rights apply all of the time. These rights include:

- **Right of 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.
- **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.
- **Right to be informed:** individuals have the right to be informed about the collection and use of their personal data.
- **Rights in relation to automated decision making and profiling:** individuals have the right not to be subject to decisions based solely on automated processing including

profiling, which significantly affects them. They can request human intervention, express their point of view and contest the decision.

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. The Data Protection Lead is responsible for the management of this.

Data Protection by Design and by Default

Outward embeds the principles of data protection by design and by default into organisational practices. Privacy and data protection is integrated into all systems, processes and decision-making from the outset. This approach ensures that only the minimum necessary personal data is collected and processed for clearly defined purposes and appropriate safeguards are in place to uphold individual's rights.
Outward takes a proactive approach to compliance to anticipate and mitigate risks before they arise.

A Record of Processing Activities (ROPA) is maintained and regularly reviewed by the Data Protection Lead. All staff have a responsibility to inform the Data Protection Lead of all new processing activities or any changes to current processing activities.

These measures help ensure that privacy is not an afterthought but a fundamental part of organisational culture and operations.

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 people we support live with others, information should always be held at 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 exposed to unauthorised access – e.g. on desks, notice boards or in insecure 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 in Outward's shared folder environment.

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 within 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 an Outward laptop/tablet.

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's 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, for example 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. If the data is in physical form, it should be destroyed appropriately upon return to the office in line with Outward's Record Management and Retention Policy.

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 external parties will usually require informed consent from the individual concerned. 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 may only be disclosed without consent if required for legal, safeguarding, or operational reasons as outlined below:

- 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 Data Privacy Impact Assessment (DPIA)

Outward must ensure a Data Privacy Impact Assessment (DPIA) is completed when it is identified that a type of data processing is likely to result in a high risk to the rights and freedoms of individuals.

Prior to processing, the project owner must inform the Data Protection Lead who will advise if a DPIA is required

A Data Privacy Impact Assessment template can be seen in **appendix 6 (AP6).**

7.4 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 a 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.

When sending postal correspondence. The correspondence address on the letter and the address on the envelope should be cross checked and verified before posting to ensure accuracy.

7.5 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 the people we support's information is therefore fundamental to providing services for the people we support's 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.
- Information may only be shared on a need-to-know basis to ensure safe and effective support and compliance with legal obligations.
- Information will not be divulged to external agencies without the person we support's informed consent unless the non-disclosure poses a serious threat of harm to the person we support themselves or to others.

7.6 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.

7.7 Maintaining confidentiality

While providing support to a person we support, 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 external party 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 their 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 Outward's Record Management and Retention Policy and ICO 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.

7.8 Artificial Intelligence (AI) Usage in Care

Whilst there are many possible use cases and potential benefits, there are also risks in using AI in care. These risks affect people drawing on care, care providers, care tech providers, and social care organisations. Risks include technological limitations (such as biased outputs or inaccurate information) and inappropriate use (such as inputting personal data, failing to collect informed consent, or not verifying outputs for accuracy and safety). Without careful oversight and transparency, AI-related risks can impact human rights, safeguarding, data privacy, security, equality, choice, control and the quality of care.

AI Usage Guidelines
Every visit to AI chatbot sites is logged by IT, and any identified data or confidentiality breaches may be subject to an investigation. When using AI tools, you must follow these three rules:

- No Identifiable Information – Avoid sharing real names, addresses, or personal details.
- Check for Quality & Accuracy – Always review AI-generated responses for correctness.
- Adhere to Policies – All existing data protection and confidentiality policies apply.

7.9 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 HR portal or otherwise in secure and lockable storage and will be accessible only to limited, relevant people.

7.10 Type of Incidents

The type of incidents, which this policy addresses, include, but is not limited to can be seen below. This list outlines common data breach incidents and incorporates lessons learned from previous occurrences at Outward.

- **IT and Data Security Incidents**

  Computers left unlocked when unattended – Employees and all users of Outward IT systems must lock their computers whenever they leave their desks. Although computers automatically lock after ten minutes, users are expected to manually lock them before stepping away.

  Password disclosures – Outward employees are assigned unique user IDs and passwords to access the organisation's systems. Staff must not share passwords under any circumstances. Any suspected or confirmed password disclosure, whether intentional or accidental, must be reported immediately.

  Phishing attempts – Clicking on suspicious emails, links, or attachments that attempt to steal login credentials or compromise security.

  Ransomware attacks – A system becoming infected with ransomware, encrypting files and demanding payment.

  Unprotected file sharing – Sending sensitive information through unsecured channels, such as personal email accounts or public cloud storage.

  Granting unauthorised staff access to shared folders – Providing access to files or systems containing sensitive data to individuals who are not authorised to view them.

- **Device and Media Security Incidents**

  Media loss – The loss, theft, or damage of portable devices such as laptops, tablets, and mobile phones. Any incident must be reported immediately to a line manager (or the on-call manager if outside working hours), as well as to Outward Facilities and the Quality team.

  ID badge loss – Staff must wear ID badges for identification purposes. If an ID badge is lost, it must be reported immediately to a line manager (or the on-call manager if outside working hours), as well as to Outward HR and the Quality team.

- **Personal Data and Confidentiality Incidents**

  Unauthorised disclosure of personal data – Personal data, including but not limited to home addresses, bank account details, and other identifiable information, must not be disclosed, discussed, or shared with unauthorised individuals.

  Sending emails to the wrong recipient – Accidentally sending personal or confidential information to unintended recipients.

Discussing sensitive information in public areas – Conversations about confidential matters being overheard by unauthorised individuals.

Inappropriate disposal of documents – Disposing of documents containing sensitive data without shredding them.

- **Physical Security Incidents**

  Unauthorised entry (tailgating) – Allowing or failing to prevent unauthorised persons from entering secured areas.

  Theft of physical documents – Losing or having printed documents containing sensitive information stolen.

  Unsecured printing – Printing sensitive documents and leaving them unattended in shared areas.

7.11 Reporting missing information, or data protection breach

Outward has a clear data breach reporting mechanism in place, detailing the procedures for reporting and recording incidents, including information security breaches.

All employees, volunteers, and contractors are required to report all incidents to the Data Protection Lead, currently held by the Outward Quality Manager and Quality team, via dataprotection@outward.org.uk, in line with the organisation's data breach reporting procedures. Reports must be submitted using the Data Breach Report Form, available on the Intranet.

Incident Reporting Timeline:
Incidents should be reported as soon as possible, ideally within 24 hours of discovery. Delays in reporting can hinder response times and increase potential harm to the organisation's assets and reputation. The Data Protection Lead and Quality will assess each case to determine if the Information Commissioner's Office (ICO) needs to be notified, in line with data protection regulations.

Serious Data Breaches:
If it becomes apparent that personal information has been misplaced, lost or accessed without authorisation, a Data Breach Report Form must be completed, and the incident must be treated as a serious breach.

The Data Protection Lead and the relevant Head of Service must be informed as soon as possible.

If a breach is likely to result in a high risk to the rights and freedoms of individuals, the Data Protection Lead will inform those concerned directly and without undue delay. The individual will be informed, in an accessible format, of:

- The nature of the personal data breach
- The contact information for the Data Protection Team
- A description of likely consequences of the breach
- Measures taken or proposed to mitigate adverse effects

If applicable, individuals will be provided with guidance on how to protect themselves from the breach's effect such as advice on how to set strong passwords and to promote vigilance against phishing attempts and fraudulent contact.

Following an internal investigation to determine whether a breach has occurred, the Executive Team will be notified of the outcome. Where necessary, appropriate reporting will be made to relevant agencies, such as the Information Commissioner's Office (ICO), Care Quality Commission (CQC) and the relevant Local Authority. All data protection incidents will be logged and monitored by the Quality Team at Outward.

7.12 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 this is to be recorded and signed on the induction checklist.

All staff will be required to undertake data protection training within the first month of their probation period and before accessing any personal data followed by mandatory refresher training every 2 years. Compliance is monitored monthly through the monthly training report and any issues raised with exec team through OPR and annual internal and external audits.

Board Members and volunteers are also required to undertake data protection training before commencing their duties.

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

7.13 International Data Transfers

In accordance with Article 44 of the UK GDPR, any transfer of personal data outside the UK must be ensured that the level of protection for individuals is not undermined. Outward will only transfer personal data internationally where appropriate safeguards are in place.

8. Responsibilities

It is the responsibility of all Outward employees, Board members and contractors to be proactive in the reporting of security incidents. It is also the responsibility of individuals and handlers of Outward data and information to ensure that all policies and procedures deal within the security and integrity of information and data are followed. All staff should complete mandatory data protection and cyber security training and compliance with this requirement will be monitored regularly.

The Data Protection Lead and Executive team members must ensure that all staff are aware of their responsibilities under this policy and are regularly updated on security risks and incidents.

9. 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

10. Implementation of the policy

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

11. Appendices

- AP1 Use of photographs/images
- AP2 Use of CCTV
- AP3 Clear desks
- AP4 Privacy Notice
- AP5 Photo/Video Consent Form
- AP6 Privacy Impact Assessment Template
- AP7 CCTV Review Form

12. 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 digitally produced or processed as part of these procedures is appropriately filed within an approved relevant filing system 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.