Registered office: Bradmere House, Brook Way, Leatherhead, Surrey KT22 7NA
www.transformhousing.org.uk | info@transformhousing.org.uk
Registered charity: 264133 | **Company limited by guarantee registered in England and Wales:** 01057984
Registered provider of social housing: H2452 | **Registered with Ofsted:** 2791302

Policy

Data Protection Policy

Policy author (name and title)	Mandy Arnold
Executive approval date	July 2026
Board / Committee approval date	Audit & Risk Committee November 2026
Review Frequency	3 years
Next review date	July 2029
Version number	1.3 – Update following recommendations from DPO Audit and minor administrative and style changes 2.0 – Updated to reflect legislative requirements of the Data Use and Access Act 2025
Has this policy been signed off by the Client Forum (if applicable)?	No
Affected	All staff

Values

Respect	**Empowerment**
▪ Value diversity and fairness ▪ Act with honesty and integrity ▪ Treat people with care and compassion	▪ Support the needs of each individual ▪ Encourage personal development and independence ▪ Provide safety, stability and security
Responsibility	**Excellence**
▪ Work together, in partnership ▪ Take responsibility for our actions ▪ Continue learning and improving	▪ Provide a first-class service ▪ Deliver excellent value for money ▪ Explore innovative ways of working

Related policies

- Information Security Policy
- Clear Workstation policy
- CCTV Policy
- Confidentiality Policy

Contents

1. Policy Statement 3
2. Responsibilities 4
3. Data Protection Policy 6
4. Principles of Processing: Fair, Lawful and Transparent Processing 6
5. Other principles of data processing 8
6. Glossary of terms 16

Procedures (available separately)

- Privacy Notice
- Retention Schedule and Procedures
- Special Categories of Personal Data
- Data Protection Impact Assessments
- Data Subjects Rights
- Data Breach Notification Procedure
- Data Processor Procedure
- Data Sharing Procedure
- International Data Transfer
- Data Protection Complaints

- Appendix 1.1 Privacy Notice (External)
- Appendix 1.2 Privacy Notice (Internal)
- Appendix 1.3 Website Privacy Notice

- Appendix 2 Retention Schedule

- Appendix 3 Data Protection Complaints Flowchart

1. Policy Statement

Transform is committed to compliance with all relevant Data Protection Legislation. We will maintain a suite of documents setting out how we intend to implement management controls to ensure legal compliance with Data Protection Legislation. We will ensure that these documents are reviewed periodically to:

a) test their adequacy in meeting the legal standards as they change over time, and
b) to test our compliance with them.

This policy has been updated to reflect the Data (Use and Access) Act 2025 (DUAA), strengthening individuals' rights in relation to personal data, including the right to raise complaints and receive a timely and transparent response.

We will ensure that all colleagues and/or other persons we commission to process personal data on our behalf, either directly or indirectly, have received appropriate and sufficient training in the application of our policies.

The Executive Team will ensure that sufficient and appropriate resources are available to ensure that we meet both our legal obligations in respect of Data Protection Legislation and the standards we set through our policies.

The Executive Team will ensure that we work within the 7 data protection principles and that we implement sufficient controls to ensure that we can demonstrate compliance with the Data Protection Legislation. This will include maintaining sufficient records of data processing activities, risk assessments and relevant decisions relating to data processing activities.

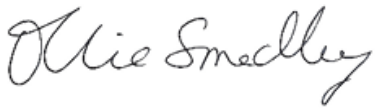
We will uphold the rights and freedoms of people conferred on them by the Data Protection Legislation. We will ensure that those rights and freedoms are appropriately considered in the decisions we take which may affect people. We will ensure that we have sufficient controls in place to assist people who wish to exercise their rights.

We are committed to being open and transparent about how we use personal information. This policy, together with our Privacy Notices and supporting procedures where appropriate, will be made available to clients, staff, volunteers and other stakeholders.

This policy applies to all our activities which involve the processing of personal data. It should be read in conjunction with the Information Security Policy

This policy applies to anyone who is engaged to process personal data for or on our behalf including: employees, volunteers, casual and temporary staff, Trustees and Committee members, involved clients, and third parties such as sub-contractors and suppliers, and anyone who we share or disclose personal data with/to.

Signed by



Chair

Date July 2026

2. Responsibilities

Data Controller
Transform Housing & Support ('**Transform**' '**We' 'Us' 'Our'**) is/are the legal data controller under the Data Protection Legislation.

The Board is responsible for approving our Data Protection Policy and gains assurance, through the Audit & Risk Committee, of our compliance with the legislative requirements.

Data Protection Officer (DPO) – the Audit & Risk Committee will appoint an independent person who will be responsible for data protection compliance. The DPO will report directly to the Committee and make recommendations as appropriate. We have appointed Data Protection People as our external DPO.

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

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

Senior Leadership Team and Line Managers
Heads of Service and Line Managers are responsible for ensuring that all data processing under their control or responsibility or commissioned by them is undertaken in compliance with this policy and other relevant data protection policies and procedures. They are responsible for ensuring that all individuals processing data understand this policy, complete iHasco online training during induction and annually thereafter, and are adequately trained to perform their duties in compliance with the policy. They oversee effective information management and security for Transform, ensuring compliance with the Data Protection Act 2018, General Data Protection Regulations 2018 and the Computer Misuse Act 1990.

Senior Information Risk Officer (SIRO)
The Head of Governance and Assurance will be the SIRO to lead and implement the information governance risk assessment programme. They will advise the Board and the Audit & Risk Committee on the effectiveness of information risk management across Transform.

The SIRO will also be responsible for maintaining the policies, guidance and training needed to ensure we are compliant with Data Protection Legislation. The SIRO will monitor and report to the senior management in respect of compliance with the policy, arrange for the investigation of any security incidents, and maintain suitable records of processing activities.

The SIRO will monitor the evolution of the Data Protection Legislation, case law, guidance, and codes of practice and incorporate relevant changes into our policy in a change-controlled manner.

The SIRO is responsible for oversight of data protection complaints, including:

- maintaining a Data Protection Complaints Register
- ensuring complaints are investigated and responded to in line with statutory timescales
- monitoring themes, risks and trends arising from complaints
- reporting outcomes and learning to senior management and the Audit & Risk Committee.

The Data Protection, Performance & Project Manager will assist with the management of data protection obligations, including maintain suitable records of processing activities.

Information Asset Owners
Information Assets and the data processing activities performed upon them are managed by nominated job roles or individuals. The **Executive Team** will ensure that an **Information Asset Owner** is assigned to each information asset and data processing activity or operation. The **Information Asset Owner** has primary operational responsibility for compliance with data protection legislation and good practice in respect of assigned information assets and processing activities.

A list of our data processing activities are set out in our Register of Processing Activities or Information Asset Register, this includes things such as completing a referral form, sending correspondence to clients, updating Pyramid notes, processing applications for employment and maintaining colleagues records, completing forms which contain any personal data.

Information Asset owners are responsible for understanding what personal data is used in their business area and how it is used, who has access to it and why. As a result, they understand and address risks to the data and us. Where the nature of our activities is such that personal data is processed as part of a single business process, across a number of separate departments, responsibility for the business process as a whole may be assigned to one named Information Asset Owner.

The **SIRO** will maintain a list of **Information Asset Owners** and the data processing activities they are responsible for in the Data Protection Register. **Senior Leadership Team** are responsible for notifying the SIRO of any new data processing activities to be added to the register as they arise.

Information Asset Owners may delegate day-to-day responsibility for compliance within their teams, ensuring that all staff are appropriately trained.

Asset Management
The Director of Asset Management, Decarbonisation & Growth has operational responsibility for compliance with data protection policies and best practice in relation to asset management policies and procedures including repairs, contractor appointment and management.

Client Services
The Director of Client Services has operational responsibility for compliance with data protection policies and best practice in relation to client policies and procedures including housing management, support services and fundraising activities.

Finance
The Director of Finance has operational responsibility for compliance with data protection policies and best practice in relation to finance policies and procedures including creditors and debtors and payroll.

People Management
The Director of Corporate Services has operational responsibility for compliance with data protection policies and best practice in relation to people policies and procedures including recruitment and retention.

In liaison with the **SIRO** Directors are responsible, through the staff performance management framework, for ensuring that adequate training is provided to all employees to ensure data protection compliance.

ICT Management
The Head of Digital and Information Services holds operational responsibility for compliance with data protection legislation and best practice for information security, and cyber security developing and reviewing the Information Security Policy (ISP).

Colleagues, volunteers, casual/temporary workers, Trustees, Committee members and officers
Anyone who is directly engaged by us to undertake data processing activities, including but not limited to, colleagues, volunteers, casual/temporary workers, Trustees and Committee members and officers etc. involved in the receipt, handling or communication of personal data must adhere to this policy. Anyone who is not confident in or has concerns about data handling practices that they carry out or see,

should contact the SIRO. Individuals are expected to complete appropriate training from time to time. Everyone within Transform has a duty to respect data subjects' rights to confidentiality.

Disciplinary action and / or penalties could be imposed on staff for non-compliance with relevant policies and legislation.

Partner and Third-Party Responsibilities
Any Third Party or organisation that is commissioned to process data or receives data from us or is able to access any personal data which is within our care of **must** enter into a legally enforceable agreement with us. The nature of this will be determined by the level of involvement with the data that is held/shared/accessed. Any such agreement must be approved by the SIRO.

3. Data Protection Policy

Introduction
We have a legal obligation to comply with all appropriate legislation with respect to data security and information governance.

This Policy sets out how we aim to meet these legal obligations concerning confidentiality and information security standards. These obligations are set out in the **UK General Data Protection Regulation (UKGDPR)**, Data Protection Act 2018, and other regulations on data protection and data privacy (such as Fundraising Regulator regulations covering charity fundraising and Privacy and Electronic Communication Regulations (PECR) 2003 covering electronic communication).

This policy has been updated to reflect the Data (Use and Access) Act 2025 (DUAA), strengthening rights, transparency and accountability in how personal data is handled.

Transform's Board and management recognise that the processing of personal data poses potential risks to the rights and freedom of the data subjects (mainly clients, colleagues and donors) whose information we collect and process. We therefore take a risk-based management approach to data management to ensure that these risks are effectively managed.

The Information Commissioner's Office (ICO) is the regulator responsible for ensuring that organisations comply with the data protection regulation. The ICO has a range of powers including the power to investigate, to issue warnings and reprimands, to order compliance, to ban processing and to suspend data flows through to imposing fines (a maximum fine of up to £17.8m or 4% of global turnover, whichever is the greater).

4. Principles of Processing: Fair, Lawful and Transparent Processing

We will ensure that processing of personal data will be done in a fair, lawful and transparent way as set out below.

4.1 **Fairness**
This ensures that the data subject is clearly informed of data held and is never knowingly misled. We will not carry out or commission data collection activities without an appropriate **privacy notice** being provided to the person from whom data is being collected and to the people who the data is about, if personal data are collected from sources other than the data subject.

Where data processing is voluntary, we will make clear the choice, risks and rights attached to the data processing and how the rights can be exercised.

The **Information Asset Owners** are responsible for ensuring that data subjects are issued with a privacy notice at the point that their data is captured.

The Executive Team will be responsible for approving the Privacy Notice and any changes to it.

Details about the content of the privacy notice and when this needs to be issued are set out in Section 7. The privacy notice is set out in **Appendix 1**.

4.2 **Lawfulness**

No data collection activities will be undertaken or commissioned without a lawful basis for the data processing activities intended to be applied to the personal data.

UKGDPR specifies a number of lawful bases for processing personal data. Before personal data is processed, the appropriate lawful basis must be identified, documented and communicated through the relevant privacy notice.

The relevant **information asset owner** will ensure the adequacy of the lawful processing of data. These seven principles are

1. **Consent** – that we can show that an individual has performed a clear affirmative action (such as answering "yes" to a question or ticking an opt-in box) to allow us to process their personal data for a specific purpose. The act sets out a specific definition for consent (art.4(11)) and specific requirements for valid consent (art.7) that will need to be considered where consent is relied upon (see paragraph 6.9).
2. **Contract** – that the data processing is necessary for a contract that we have with the individual.
3. **Legal Obligation** – that the data processing is necessary for us to comply with the law. The relevant legislation will be cited and appropriately documented.
4. **Vital interest** – that the data processing is necessary to protect someone's life.
5. **Public task** – that the data processing is necessary to perform a task in the public interest or to carry out an official function. A Public Interests Assessment (PIA) will be undertaken and documented.
6. **Legitimate Interest** – that the data processing is necessary for our legitimate interest or the legitimate interest of a third party unless the interests or rights and freedoms of the individual override those interests. A Legitimate Interests Assessment (LIA) will be undertaken and documented.
7. **Recognised Legitimate Interest** - this applies to specific processing activities defined in legislation, including safeguarding, prevention and detection of crime, and emergency response. Where this basis applies, we are not required to carry out a balancing test, but must still ensure that processing is necessary, proportionate and transparent. Where Transform relies on a Recognised Legitimate Interest, the Information Asset Owner must document the rationale, category relied upon and why the processing is necessary and proportionate.

For specific information regarding the lawful basis for processing Special Categories of Protected Data (SCPD) including criminal and conviction data (see paragraph 5.7).

There is no order of importance to the lawful bases above. You must take care when determining which lawful basis to use as some may not be applicable and others have certain conditions attached. Which basis is more appropriate will depend on the purpose for the data processing and the relationship that we have with the individual. We must determine the lawful basis before processing the data and this has to be disclosed in the privacy notice.

Information Asset Owners, in consultation with the **SIRO**, are responsible for ensuring that there are lawful grounds for all data processing activities that fall under their control, that the consent policy is adhered to, and a LIA/PIA is properly undertaken where necessary.

The **Data Protection, Performance & Project Manager** will maintain a register of the lawful grounds for all of our processing activities involving the processing of personal data, as approved by the SIRO, in the Information Asset Register.

4.3 **Transparency**

We will endeavour to provide sufficient information about how personal data is being processed to enable sufficient transparency about its handling of personal data. The **SIRO** will periodically review the transparency arrangements.

Where automated decision-making is used, we will provide clear and meaningful information to individuals about how decisions are made and their rights in relation to those decisions.

This includes clear information on the right to raise a data protection complaint and how to do so, as set out in our Privacy Notice and published on our website.

5. Other principles of data processing

5.1 **Purpose of Data Processing**

We must establish a clear purpose for which the personal data is being collected. This information must be included in the privacy notice as well as in the retention procedure. The **information asset owners** need to ensure that the data is not used for any other purpose than the one stated. The **SIRO** oversees the maintenance of a Register of Processing Activities (ROPA) or Information Asset Register. Any new data processing activities require the approval of the **SIRO**. The **Data Protection, Performance & Project Manager** is responsible for creating and updating the register. The register will be reviewed by the **Senior Leadership Team.**

5.2 **Data adequacy and minimisation**

We must use the minimum personal data as practically possible in our processing activities and ensure that the personal data collected is adequate for the identified purpose. We recognise the strict requirements on data profiling under UKGDPR and that any data matching and profiling of personal data with other information must comply with UKGDPR requirements to be lawful.

Information asset owners are responsible for ensuring that no unnecessary, irrelevant, or unjustifiable personal data is collected as part of their data processing activities.

5.3 **Data Quality**

We recognise the need for the personal data to be accurate, complete and, where necessary, kept up to date so that stakeholders can have confidence in us and our decision-making process. The data subject has the right to rectify any incorrect personal information.

We take a risk-based approach to data processing, which means that data should be:

- **Accurate** - data should be sufficiently accurate for the intended purpose. Data should only be captured once, although it may have multiple uses. The importance of the 'uses of the data' should be balanced with the 'costs and the efforts of correction'. Where compromises are made on the data accuracy, the resulting limitations of the data should be made clear.
- **Valid** - data should be recorded in an agreed format.
- **Reliable** - data should reflect a stable and consistent data collection process.
- **Timely** - data should be available within a reasonable time, rapidly and frequently enough to support the information needs.
- **Complete** - all data should be captured in accordance with agreed definitions and information needs. Monitoring missing, incomplete or invalid data elements provides an invaluable measure of data quality.

We recognise that certain data is more important to keep accurate and up to date than others. For example, keeping client contact details such as address and telephone number up to date is a high priority otherwise it may have a detrimental impact on the data subject.

Any personal data that cannot reasonably be assumed to be accurate and up to date will be treated appropriately through erasure or anonymisation to reduce any data risk.

Information Asset Owners are responsible for ensuring that personal data they have collected or created through their data processing activities are kept accurate and up-to-date or deleted or anonymised.

5.4 **Data Retention**

We must ensure that we do not retain personal data for any longer than is necessary for legal or regulatory purposes or for its legitimate organisational interest. Given this, we must set time limits for the periodic review and erasure (or deletion) of personal data as appropriate.

The Data Retention Schedule sets out the retention periods for different types of documents to ensure timely and appropriate disposal of data and what needs to happen to it at the end of its useful life. Retention periods for information assets are made publicly known to the data subjects at the time of data collection, in accordance with our Privacy Notice. The procedures are set out in **Section 8**.

SIRO will maintain a data retention schedule setting out approved retention periods and end of life treatment.

Information Asset Owners are responsible for:

- determining the retention period for personal data under their control, with advice from the SIRO and DPO.
- ensuring that the retention schedules and disposal procedures for their respective information assets are communicated to colleagues.
- Reviewing personal data held against the retention schedule on a continuous basis to ensure that any personal data no longer required is securely anonymised or erased in accordance with the end-of-life data procedure.
- Ensuring that no personal data is retained beyond the identified retention period unless agreed with the SIRO as a justifiable extension which complies with data protection legislation.
- Where data is archived (or otherwise transferred for long terms preservation) carry out a risk assessment to ensure appropriate measures such as data minimisation, encryption and anonymisation are applied to safeguard the data.

The **Head of Digital and Information Services**, working with the outsourced IT provider, LIMA, will ensure that personal data held in a digital form is centrally managed and, where appropriate, is erased in compliance with this policy.

5.5 **Information Security**

We must ensure that personal data is processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical and organisational measures.

An information security policy (ISP) will be maintained setting out specific policies which aims to protect personal data and limit access to it by only with those with authority to access it. The **Head of Digital and Information Systems** will be responsible for the formulation of the ISP and will develop and maintain this in consultation with the **SIRO**. The ISP will be approved by the Board.

5.6 **Children's data**

We must take special measures if we process personal data relating to children under the age of 13 including the nature of privacy information provided and approach to information rights requests. We do not house or support clients under the age of 16 although we may hold personal data about some clients' children. We will ensure that adequate safeguards are in place to protect this personal data.

If we provide information services (digital services) that might be used by people under the age of 18, the **SIRO** will consider the applicability of the Age-Appropriate Design Code of Practice and make provisions accordingly. Further guidance available here.

Where services may impact children, we will consider their specific protection needs, including their vulnerability, level of understanding, and the risks associated with processing their data.

5.7 **Special Categories of Personal Data**

Special categories of personal data (SCPD) are personal data revealing:

- racial or ethnic origin,
- political opinions,
- religious or philosophical beliefs,
- trade union membership,
- the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person,
- data concerning health,
- data concerning a natural person's sex life or sexual orientation.

Other forms of sensitive data include data about gender identity and criminal allegations, proceedings or convictions. When referring to SCPD throughout this policy, this is understood to include these other forms of sensitive data.

The processing of SCPD is prohibited by Article 9(1) of the UKGDPR unless certain conditions set out in Articles 9(2) to 9(5) are met which are further defined in Schedule 1 Part 1 of the DPA18.

We rely on conditions provided under section 10 of the Data Protection Act 2018 whenever we process SCPD data. This requires that we maintain an appropriate policy in accordance with Schedule 1, Part 4 of the DPA 2018.

We will not process SCPD unless it is necessary. No SCPD data will be processed by us unless approved by SIRO. Where the processing of SCPD is necessary, the **SIRO** will ensure that the lawful grounds for such processing are documented and will maintain a periodic review of the necessity to processing the special categories of personal data.

Managers are responsible for ensuring that this policy is shared with, and made readily available to, all new employees and data processors that we plan to commission. The latest version will be made available on Milo and our website.
We will ensure any relevant third parties we commission to process SCPD data on its behalf understands their responsibilities under GDPR. The information asset owner should ensure that this is assessed as part of the due diligence carried out for that data processor.

Further information about processing SCPD are set out in the **SCPD Procedure**.

5.8 **Personal data relating to criminal convictions and offences**

If we are processing personal data relating to criminal convictions and offences of clients or staff we will process it in the same manner as Special Categories of Personal Data (See paragraph 5.7).

5.9 **Consent**

We will interpret consent to be as defined in the UKGDPR and that any consent will not be valid unless:

- there is a genuine choice of whether or not to consent.
- it has been explicitly and freely given, and represents a specific, informed and unambiguous indication of the data subject's wishes that indicates agreement to the processing of personal data relating to them.
- the consent was given through a statement made by the data subject or by a clear affirmative action undertaken by them.
- we can demonstrate that the data subject has been fully informed about the data processing to which they have consented and are able to prove that it has obtained valid consent lawfully.
- we make provisions so that data subjects can withdraw consent, being as easy to withdraw as it was to give, informing the data subject has about how to exercise their right to withdraw consent.

We recognise that consent may be rendered invalid if the above points cannot be confirmed or if there is an imbalance of power between the data controller and the data subject. We recognise that consent cannot be considered to last forever and will determine a consent refresh period for every instance where consent is the lawful condition for processing.

Where consent is the lawful basis for processing, the **Information Asset Owners** will ensure that consent is properly obtained in accordance with the conditions above.

UKGDPR does not indicate a shelf life for consent. Theoretically, a person's consent is indefinite, though there might be situations in which it becomes clear that consent is no longer valid or reasonable or violates some principle of data processing. However, a data subject has the right to withdraw consent at any time.

5.10 **Record keeping and accountability**

We will maintain an appropriate accountability framework including records of processing activities, data protection impact assessments, complaints, breaches, lawful basis assessments, data sharing arrangements and processor oversight records sufficient to demonstrate compliance with Data Protection Legislation.

The **SIRO** will be responsible for overseeing preparation the RoPAs and providing them to the Information Commissioner's Office on demand when required. The **Data Protection, Performance & Project Manager** support the SIRO in maintaining the RoPAs.

5.11 **Data Subjects' Information rights policy**

We recognise the legal rights of those whose data we are processing or intend to process and will ensure that appropriate information is provided to them advising them of their rights. Policies and procedures will be maintained to ensure that we are able to recognise information rights requests and handle them appropriately when they are exercised. These rights include:

- Right to information about data processing operations
- Right of access to personal data
- Right to portability of personal data
- Right of rectification of personal data
- Right of erasure of personal data
- Right to restriction of processing
- Right to object to direct marketing
- Right to object to data processing operations under some circumstances
- Right not to be subject to decisions made by automated processing under some circumstances
- Right to request human intervention and challenge decisions made solely by automated processing
- Right of complaint about Transform's processing of personal data and the right to a judicial remedy and compensation.

How to process these rights is covered the **Data Subject Rights (DSR) Procedure (Section 11A)** and our more detailed **Data Subject Access Rights Procedure (Section 11B)** specifically for right of access to personal data.

In line with the Data (Use and Access) Act 2025 (DUAA), we explicitly recognise the right of individuals to raise complaints about how their personal data is processed and to receive a timely and transparent response.

We will ensure that individuals can exercise their rights free of charge unless legislation permits a fee and that requests are handled in accordance with statutory timescales.

5.12 **Personal Data Breaches**

We will maintain a Data Breach Reporting Procedure and will ensure that all employees and those with access to personal data are aware of it and this personal data breaches policy.

Everybody with access to personal data for which we are either data controller or processor

- must report all personal data breaches to their line manager and the **SIRO**
- **ensure that it is r**eported as soon as they become aware of the breach. We must report to the ICO within **72 hours after becoming aware of the breach**[1] where it is likely to result in a risk to the rights and freedoms of Individuals.

The **SIRO** will log all personal data breaches and will investigate each incident without delay. Appropriate remedial action will be taken as soon as possible to isolate and contain the breach, evaluate and minimise its impact, and to recover from the effects of the breach.

Data protection near misses will also be recorded and investigated in the same manner as data protection breaches. The Data Breach Reporting Procedure (Section 12) sets out responsibilities, decision-making criteria and timescales for notifying data subjects, the Information Commissioner and the media about a personal data breach.

5.13 **Processors**

We reserve 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 processors may be appointed who are unable to provide satisfactory assurances that they will handle personal data in accordance with the Data Protection Legislation.

Colleagues wishing to appoint a processor will ensure that appropriate due diligence is undertaken on the proposed processor to provide sufficient guarantees of technical, physical and organisational security measures and data protection compliance prior to their appointment. The **SIRO** will provide advice and guidance in respect of this.

A written agreement will be implemented between Transform and the processor which at least meets the requirements of the Data Protection Legislation. The **SIRO** will ensure that a register of such agreements/arrangements is maintained. The processor agreement will specify what is to happen to personal data upon termination of the data processing agreement. Procedures are set out in Section 12.

No colleague is permitted to commission or appoint a third party to process data on our behalf without adhering to this policy.

[1] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/#howmuchtime

5.14 **Transform as a processor**

Where we act as a processor we will ensure we retain records of processing activities which record at least the information required under Article 30(2) of the UKGDPR for each controller it acts on behalf of. We will ensure that we have an appropriate agreement in place with each data controller and will look to 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.

5.15 **Data sharing, disclosure and transfer**

We will only share or disclose personal data to other organisations and third parties where there is a legal basis for doing so and the data sharing is necessary for specified purposes. No data sharing or disclosure is permitted to occur without a suitable legally enforceable agreement satisfying the requirements for such agreements as set out in the Data Protection Legislation being in place.

Data sharing agreements must be approved by the **SIRO.** Information Asset Owners are responsible for ensuring that where Data Sharing agreements are required that these are put in place.

The **Data Protection, Performance & Project Manager** will maintain a register of all such agreements.

Appropriate risk assessments will be undertaken prior to any data sharing taking place on those with whom we intend to share personal data. This policy extends to appointing others to process personal data on our behalf, sharing personal data with organisations, and providing information to ad-hoc requests for information such as those which may be received from the police and other authorities.

We will provide information to all colleagues setting out safe and approved methods of transferring personal data to recipients.

Colleagues are required to use only approved methods of data transfers. Disciplinary action will be taken against employees who fail to observe the data transfer policy and use unsafe and insecure methods of data transfer unless such methods have been approved in writing by the **SIRO.** Procedures are set out In Section 14

5.16 **International transfer of personal data**

We will not transfer nor process nor permit personal data to be transferred or processed outside the United Kingdom without the conditions laid down in the Data Protection Legislation being met to ensure that the level of protection of personal data are not undermined. Any transfer or processing of personal data that we undertake or commission, directly or indirectly, must be approved by the **SIRO** and may only take place if one of the following is satisfied:

- The territory into which the data are being transferred is one approved by the UK Government;
- The transfer is made under the unaltered terms of the International Data Transfer Agreement (IDTA) issued by the Information Commissioner for such purposes and where required a Transfer Risk Assessment (TRA) issued by the Information Commissioner for such purposes;
- The territory into which the data are being transferred has a decision with regard the adequacy of its data protection regime (Adequacy Regulations) issued by the UK Government;
- The transfer is made under the provision of binding corporate rules which have been approved and certified by the UK Government;
- The transfer is made in accordance with one of the exceptions set out in the Data Protection Legislation.

Where necessary the **SIRO** will ensure that a risk assessment is carried out on any country outside the UK that we intend to transfer personal data to and that any safeguarding measures

are implemented as necessary to ensure adequate protection of personal data. This is detailed further in Section 15.

5.17 **Risk assessment**

We will adopt a risk-based approach to processing personal data ensuring that we assess any risks to privacy or to the rights and freedoms of people before commencing or commissioning or changing data processing activities. Where necessary we will, as a minimum, ensure that a data protection impact assessment (DPIA) is undertaken where required by Data Protection Legislation (See Section 10) and/or when one is deemed to be desirable by the **SIRO**.

We will maintain a procedure setting out how data protection impact assessments are to be carried out and documented and ensure that appropriate resources are available to advise on DPIAs. This can be found in Section 10 – DPIA Procedure.

The **SIRO** is responsible for maintaining a register of data protection impact assessments that have been undertaken by us and for its periodic review.

5.18 **Training and Awareness**

We need to ensure that all colleagues and other workers are competent in understanding the data protection responsibilities assigned to them. We will ensure these individuals are provided with appropriate training in the application of this and other data protection policies and procedures and in their data protection responsibilities. The Data Protection training module will form part of the induction programme for all colleagues and other workers and refresher training provided every year.

We will also provide data protection awareness raising activities from time to time to keep data protection front of mind. All training and awareness raising activities will be logged.

Information Asset Owners will determine the training needs of those people within their teams and that appropriate data protection awareness and training is provided. The **Director of Corporate Services** will ensure that the training is measured and reported.

5.19 **Continuous Improvement, audit and compliance checking**

We will undertake periodic compliance checks to test whether our policies and procedures are being adhered to and to test the effectiveness of our control measures. Corrective action will be required where non-conformance is found.

Records will be kept of all such audits and compliance checks including corrective action requests raised.

Disciplinary action will be taken against individuals who fail to act upon the reasonable corrective action requests properly formulated and raised through data protection audits. The Audit & Risk Committee will be provided with a summary of audit findings periodically.

Data protection complaints, associated risks and learning will be included within periodic compliance reporting and assurance reviews.

Periodic assurance reporting to the Audit & Risk Committee will include information relating to significant personal data breaches, data protection complaints, ICO correspondence, subject access requests, audit findings and emerging information governance risks.

5.20 **Data protection by design and by default**

We will strive to foster a culture of data protection by design and by default in all of our data processing activities.

We will ensure that measures are in place to encourage all those involved in data processing activities to adopt continuous improvement to the technical and organisational measures that implement the data protection principles and safeguards into processing activities.

We will strive to ensure that by default, only personal data which is necessary for each specific purpose of the processing is processed and that the extent of the processing, period of their storage and their accessibility is made clear. In particular, such measures will ensure that by default personal data is not made accessible without the individual's intervention to an indefinite number of natural persons (i.e. automated processing).

We may make use of automated decision-making, including decisions based solely on automated processing, where permitted by law. In line with the Data (Use and Access) Act 2025, such processing may be carried out in a wider range of circumstances, provided that appropriate safeguards are in place.

These safeguards will include:

- providing individuals with meaningful information about the decision
- enabling individuals to request human intervention
- enabling individuals to challenge or contest decisions

Automated decision-making will only be used where it is necessary, proportionate, and consistent with the rights and freedoms of individuals.

Prior to implementing new automated decision-making systems, a DPIA must be completed and approved by the SIRO and Data Protection Officer where the processing presents a high risk to individuals.

In particular, there are additional policies which support the Data Protection Policy to ensure we observe data protection by design and default. These are:

- CCTV Policy – where we have CCTV equipment installed or consideration is given to installing new equipment it is important that the requirements of this policy are observed by the Information Asset Owners and the Housing Services Managers responsible for the equipment.
- Clear Workspace and Screen Policy – provides information to colleagues to support them in keeping paper and electronic documents secure when working in the office, at home or in their vehicle by maintaining a clear desk, clear screen and clear vehicle.

5.21 **Complaints and enforcement**

Concerns relating to the processing of personal data must be managed through the Data Protection Complaints Process set out in Section 16 of this policy.

The general Complaints Policy does not apply to data protection complaints and we will direct individuals to this policy where appropriate. Information about our complaints policy will be included in our Privacy Notice.

6. Glossary of terms

Controller:
An individual or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. Organisations like Transform will be the data controller when they hold and use personal data relating to their clients, staff or donors.

Data erasure:
This entitles the data subject to have the data controller erase his / her personal data. Please note that there are some specific circumstances where the right to erasure of data does not apply.

Data portability:
This is the requirement for data controllers to provide the data subject with a copy of his or her data in a format that allows for easy use with another data controller. Please note that there are specific requirements to the applicability of such requests.

Retention Schedule means a document used to record the Initial Retention Period, Retention Criteria, Initial Treatment, Secondary Retention Period, Tertiary Treatment and the justification for each of these.

Data Protection Complaint A data protection complaint is any expression of dissatisfaction about how personal data is collected, stored, used, shared, retained or secured, including how we respond to data subject rights requests.

Data Protection Principles there are seven principles that guide the processing of personal data:

Lawfulness, fairness, and transparency: Data must be processed lawfully, fairly, and in a transparent manner.

Purpose limitation: Data should only be collected for specified, legitimate purposes and not further processed in a manner incompatible with those purposes.

Data minimisation: Only the minimum amount of personal data necessary for the intended purpose should be collected.

Accuracy: Personal data must be accurate and kept up to date.

Storage limitation: Data should not be kept in a form that allows identification of data subjects for longer than necessary.

Integrity and confidentiality: Data must be processed securely to protect against unauthorized or unlawful processing and against accidental loss, destruction, or damage.

Accountability: The data controller is responsible for demonstrating compliance with these principles.

Data Protection Officer (DPO)
An expert on data privacy who works independently to ensure that we are adhering to the policies and procedures set out in the GDPR. We have commissioned The Data Protection People to act as our DPO.

Data subject:
Defined under the UKGDPR as 'any information relating to an identified or identifiable living individual.

Data Subject Rights:
UKGDPR gives data subjects the right to:

- Transparency (to be informed)
- Access the data held on them
- Rectify the data if it is incorrect
- Request that the data be erased (or be forgotten)
- Restrict processing

- Data portability
- Object to the processing of data
- Not to be subject to a decision based solely on automated processing

Identifiable living individual:
A living individual who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data or an online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual.

Information Asset Owners (IAO):
These are the Senior Leadership Team members responsible for their key areas within the organisation.

Information Asset Register (IAR):
This is a document listing all information held or processed by us. It is sometimes also referred to as a Record of Processing Activities (RoPA) as required by Article 30 of the UKGDPR; and for the purposes of this policy the two terms should be regarded as synonymous.

Information Governance Framework:
The framework sets out the various registers and logs where records are kept which demonstrates our compliance with Data Protection Legislation.

This list of registers that are maintained are:

A. Register of Processing Activities and Information Asset Register
B. Register of Data Breaches (and near misses)
C. Register of Data Privacy Impact Assessments (DPIAs)
D. Register of Subject Access Requests and other rights requests
E. Register of Processors
F. Register of Data Sharing
G. Data Retention Schedule
H. Register of Data Protection Complaints

Information Incident:
An identified occurrence or weakness indicating a possible breach of information security or failure of safeguards, or a previously unknown situation which may be relevant to the security of information.

Lawful basis
For any personal data processed, we must be able to specify that it has been processed on one of the legal grounds specified by GDPR. UKGDPR provides six lawful bases for processing personal data:

- Individual's consent
- Contract with the individual
- Complying with a legal obligation
- If it is in the vital interest of the data subject
- If it is necessary for a task in the public interest or authority
- We may process personal data where it is necessary for a legitimate interest, including a Recognised Legitimate Interest defined by legislation.

For SCPD the lawful grounds are found within art.9(2) – see Section 9.
For Criminal Conviction data the lawful grounds are found in DPA18 schedule 1 – see Section 9.

For much of our work, the legal basis will be the contract with the data subject.

Personal data:
Any information relating to an identified or identifiable living individual. This includes name and address but could also include contact details or even IP address. It should be remembered that one or more

non-specific pieces of information, when combined, could identify a specific individual. For example, a combination of gender, date of birth and geographic indicator might identify a specific individual.

Personal data breach:
A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Processing personal data:
Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Processor:
An individual or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

Profiling:
Any form of automated processing of personal data intended to evaluate certain personal aspects relating to a natural person, or to analyse or predict that person's performance at work, economic situation, location, health, personal preferences, reliability, or behaviour. This definition is linked to the right of the data subject to object to profiling and a right to be informed about the existence of profiling, of measures based on profiling and the envisaged effects of profiling on the individual.

Recipient:
An individual or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not.

Register of Data Protection Complaints:
A central record to log, monitor, investigate and report complaints relating to the processing of personal data. The register records key information such as the nature of the complaint, dates received, actions taken, outcomes, lessons learned and any remedial measures implemented. It supports accountability, regulatory compliance, trend analysis and service improvement in relation to data protection matters.

Retention Period:
This means the period of time that personal data are stored in a format which permits the identification of individuals.

Retention Criteria:
This means the criteria used to determine the Retention Period which can include a prescribed period of time (eg 7 years from the date of a record's creation), or a trigger point (eg 2 years after the closure date of a case).

Risk:
The chance of something happening, which will have an impact upon objectives. It is measured in terms of likelihood of an event happening and the consequences if the risk materialises.

Risk management:
The culture, processes and structures that are directed towards the effective management of potential opportunities and adverse effects.

Senior Information Risk Officer (SIRO)
This is the person who acts as a strategic leader for information governance and for day-to-day data protection compliance. For us, the SIRO is the Head of Governance & Assurance.

Special categories of personal data:
Special categories of personal data ("SCPD") are defined as:

- personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership.
- genetic data or biometric data processed for the purpose of uniquely identifying a natural person.
- data concerning health or
- data concerning a natural person's sex life or sexual orientation.

Due to the sensitivity of this data, the processing of SCPD is prohibited by Article 9(1) of the UKGDPR unless certain conditions set out in Articles 9(2) to 9(5) are met which are further defined in Schedule 1 Part 1 of the DPA18. Other forms of sensitive data include data about gender identity and also criminal allegations, proceedings or convictions. When referring to SCPD throughout this policy, this is understood to include these other forms of sensitive data.

Subject Access Right:
This entitles the data subject to have access to the information that a data controller has concerning them. Our data subjects can request access to their personal data by completing a Data Subject Access Request (DSAR) form.

Third Country:
This means a territory that is not the United Kingdom in the UKGDPR.

Third Party:
An individual or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

Treatment:
This means the processing applied to personal data at the end of the Retention Period (eg erasure, pseudonymisation, anonymisation).