Data Protection Policy

Approved 24 February 2022

BIELD
FREE TO BE

Title of Policy	Data Protection Policy
Approved by	Board
Approval Date	24/02/2022
Owner	Director of Customer Experience
Author	Head of Policy and Customer Standards
Version	2.0
Period of Review	60 months
Date of Review	25/02/2027
Lead Directorate	Customer Experience
Stakeholders	☐ Partnership Forum ☒ Human Resources ☒ ICT ☐ Staff Forum ☒ Property ☐ Other ☒ Finance ☒ BR24 ☒ Operations ☒ Business Development
Scottish Social Housing Charter Outcomes and Standards this policy helps to achieve	☒ Outcome 1 ☐ Outcome 6 ☐ Outcome 11 ☐ Outcome 2 ☐ Outcome 7 ☐ Outcome 13 ☐ Outcome 3 ☐ Outcome 8 ☐ Outcome 14 ☐ Outcome 4 ☐ Outcome 9 ☐ Outcome 15 ☐ Outcome 5 ☐ Outcome 10
Care Standards this policy helps to achieve	☐ Standard 1 ☐ Standard 2 ☐ Standard 3 ☒ Standard 4 ☐ Standard 5
Bield Objectives this policy helps to achieve	☐ Objective 1 ☒ Objective 3 ☐ Objective 5 ☐ Objective 2 ☒ Objective 4 ☐ Objective 6

What you will find in this policy

1 Introduction

1.1. Our vision is a Scotland where people of all ages are respected can make their own choices and lead independent and fulfilling lives.

1.2. Our mission is to improve the quality of life of older people by offering a diverse range of housing, care, and other services.

1.3. This policy embodies our values, which are:

Honesty	Equality and Diversity	Ambition	
Dignity	Integrity	Caring	Kindness

1.4. To help us achieve our mission, we need to gather and use certain information about individuals.

1.5. These can include

- customers (tenants, factored owners, etc.) and their families
- colleagues
- Board and committee members
- other individuals that Bield has a relationship with.

1.6. As a result, we manage a significant amount of data, from a variety of sources.

1.7. This data contains Personal Data and Sensitive Personal Data (known as Special Categories of Personal Data under the GDPR).

1.8. We are committed to ensuring the secure and safe management of data we hold concerning customers, colleagues, and other individuals.

1.9. This policy sets out our duties in processing that data, and the purpose of this policy is to set out the procedures for the management of such data.

1.10. Employees, volunteers, and members of Bield's Board of Management and Committees have a responsibility to ensure compliance with the terms of this policy and to manage individuals' data following the procedures outlined in this policy and associated documentation.

2. Policy Outcomes

2.1. The purpose of this policy is to:

- Provide clarity on our approach to data protection for our customers, colleagues, and Board members
- Protect personal data and sensitive personal data of our customers, colleagues, and other stakeholders
- Reduce the opportunity for security breaches

2.2. Any failure to comply with the Policy may breach confidentiality and will expose us to a potential breach of customer, stakeholder, partner, and/or supplier trust.

2.3. A breach of this Policy may also result in or contribute to theft of intellectual property, fraud, and/or identity theft.

2.4. Furthermore, failure could constitute a breach of our legislative, regulatory, and/or contractual requirements including our statutory obligations under the Data Protection Legislation, which could also result in a fine and/or court action against us.

2.5. There are benefits to embedding compliance with the Data Protection Principles into our culture

2.6. These include:

- protecting the rights and interests of individuals (such as our tenants and their families, our service-users, and colleagues) whose personal information we hold
- supporting good governance
- promoting business efficiency and underpinning service delivery
- supporting compliance with other legislation and regulations which requires personal information to be processed following the Data Protection Principles
- improving accountability and enabling compliance with the Data Protection Legislation and other rules and requirements to be demonstrated
- protecting the rights and interests of stakeholders
- protecting our reputation and brand image
- protecting our assets.

3. Equality, Diversity, and Inclusion

3.1. When carrying out this policy we will adhere to our Equality and Diversity Policy which aims to promote diversity, fairness, social justice, and equality of opportunity. An Equality Impact Assessment was carried out concerning this policy and this is included in Appendix 1.

3.2. In addition to the points made above, to help promote equality and inclusion, the following steps will be taken for this policy:

- Large print version
- Translation and interpretation message on the back of the policy
- Easy to read version for people with mental impairment

4. Definitions

4.1. Key terms that are often used concerning data protection are outlined below.

Consent
Any freely given, specific, informed, and unambiguous indication of the data subject's wishes by which they, by a statement or by clear affirmative action, signifies agreement to the Processing of personal data relating to them.

Controller
The organisation that determines the purposes and means for processing personal data.
Personal Data.

Data protection officer (DPO)
A Data Protection Officer (DPO) is an individual who has an over-arching responsibility and oversight over compliance with Data Protection laws.

Data protection principles
The data protection principles under the GDPR.

Data subject
Any person who can be identified, directly or indirectly, via an identifier such as a name, an ID number, location data, or via factors specific to the person's physical, physiological, genetic, mental, economic, cultural, or social identity.

Personal information
Any personal data that relates to and identifies (either directly or indirectly) an individual from information that is held by us.

It also includes any expression of opinion or view about an individual or their circumstances. Examples of personal data relating to individuals include their:

- name
- age

- date of birth
- contact details
- marital status
- housing history
- financial status
- allowance, benefits, and grants claimed.

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, eg accidental loss, destruction, theft, corruption, or unauthorised disclosure of personal data.

Processing
Any activity that involves the use of personal data, including:

- obtaining
- recording
- holding
- organising
- amending
- retrieving
- using
- disclosing
- erasing
- destroying

Sensitive personal data or special category personal data
personal data which the GDPR says are more sensitive, and so needs more protection. This includes data relating to:

- race or ethnic origin
- political opinions
- religious or other beliefs of a similar nature
- physical or mental health or condition
- trade union membership
- sexual life or sexual orientation
- genetic or biometric data where

5. Data

5.1. We hold a variety of data relating to individuals, including customers and employees (also referred to as data subjects) which is known as Personal Data.

5.2. The personal data we hold and process is detailed within the Fair Processing Notice in Appendix 2 (see Section 7.4). It is also included in the Data Protection Addendum of the Terms of and Conditions of Employment which has been provided to all employees.

5.3. We also hold personal data that is sensitive (ie relates to or reveals a data subject's racial or ethnic origin, religious beliefs, political opinions, health, or sexual orientation. This is "Special Category Personal Data" or "Sensitive Personal Data".

6. Data protection principles

6.1. As an organisation, we are required by law to adhere to and demonstrate compliance with the following principles:

Processed properly
Personal data must be processed lawfully, fairly, and transparently about individuals

Legitimate purpose
Personal data must be collected for specified, explicit, and legitimate purposes, and not further processed in a manner that is incompatible with those purposes

Limited
Personal data must be adequate, relevant, and limited to what is necessary for the purposes for which they are processed

Accurate
Personal data must be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that inaccurate personal data, having regard to the purposes for which they are processed, are erased or rectified without delay

Time-bound
Personal data must be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed

Secure
Personal data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and accidental loss, destruction, or damage, using appropriate technical or organisational measures.

7. Processing personal data

7.1. We are allowed to process personal data on behalf of data subjects provided it is doing so on one of the following grounds:

- Processing with the consent of the data subject (see Section 7.4)
- Processing is necessary for the performance of a contract between us and the data subject or for entering into a contract with the data subject
- Processing is necessary for compliance with a legal obligation
- Processing is necessary to protect the vital interests of the data subject or another person
- Processing is necessary for the performance of a task carried out in the public interest or the exercise of our official authority
- Processing is necessary for legitimate interests

Fair Processing Notice

7.2. We have a Fair Processing Notice (FPN) which we are required to provide to all customers whose personal data we hold.

7.3. The FPN must be provided to the customer from the outset of processing their data and they should be advised of the terms of the FPN when it is provided to them.

7.4. The Sample Fair Processing Notice in Appendix 2 sets out the personal data we process and the basis for that processing.

Employees

7.5. We hold and process employee personal data and, where applicable, special category personal data or sensitive personal data.

7.6. Details of the data held and processing of that data are contained within the Employee Fair Processing Notice which is provided to Employees at the same time as their Contract of Employment.

7.7. A copy of any employee's Personal Data held by Bield is available upon written request by that employee.

Consent

7.8. Consent as a ground of processing will require to be used from time to time when processing personal data. It should be used where no other alternative ground for processing is available.

7.9. If we are required to obtain consent to process a data subject's data, it shall be obtained in writing. The consent provided by the data subject must be freely given and the data subject will be required to sign a relevant consent form if willing to consent.

7.10. Any consent to be obtained must be for a specific and defined purpose (i.e. general consent cannot be sought).

Processing of special category personal data or sensitive personal data

7.11. The processing of special category personal data or sensitive personal data must be done in line with one of the following grounds of processing:

- The data subject has given explicit consent to the processing of this data for a specified purpose
- Processing is necessary for carrying out obligations or exercising rights related to employment or social security
- Processing is necessary to protect the vital interest of the data subject or if the data subject is incapable of giving consent, the vital interests of another person
- Processing is necessary for the establishment, exercise, or defence of legal claims, or whenever courts are acting in their judicial capacity
- Processing is necessary for reasons of substantial public interest.

8. Authorised sharing of information

8.1. In certain circumstances (and subject strictly to conditions set out in the Data Protection Legislation) personal information may be shared by us with other organisations and partners.

8.2. This may occur, for example by way of:

- A reciprocal exchange of information
- Different parts of the same organisation making information available to each other
- One or more organisations providing information to third party or parties
- Several organisations pooling information and making it available to each other
- one-off disclosures in unexpected or emergencies

8.3. Personal information may be shared systematically, for example, by way of the routine sharing of information for an agreed purpose(s). Where this occurs, this must be underpinned by adherence to strict conditions and procedures to be governed by a data-sharing agreement.

8.4. We may decide, or be asked, to share personal information in situations that are not covered by the routine agreement.

8.5. In some cases, this might involve a decision about sharing in 'one-off' circumstances. This might include an emergency.

8.6. Before we can share personal information we must consider all of the legal implications of doing so, not simply the terms of the Data Protection Legislation. Appendix 3 Key considerations for sharing data sets out key issues that must be taken into account before a decision is made whether it is appropriate to share personal information.

Freedom of Information and Environmental Information Regulations

8.7. We are subject to the terms of the Freedom of Information (Scotland) Act 2002 (FOISA) and the Environmental Information (Scotland) Regulations 2004 (the EIRs). These provide individuals with the right of access to any information held by us. Where a request is made under FOISA or the EIRs for personal information, this may be disclosed if the disclosure would not contravene any of the Data Protection Principles.

8.8. We are fully committed to the aims of FOISA and the EIRs and will make every effort to meet our obligations.

Requests relating to legal proceedings

8.9. We are sometimes requested to disclose personal information to other public sector organisations and by law firms in connection with legal proceedings. Such requests should be passed to the Data Protection Officer who will consider the following:

- If the request has authority to request the information, for example, if a mandate is required
- If there are any applicable exemptions
- What privacy notice information has been provided to the individual in question and if this is sufficient to cover the proposed disclosure in compliance with the first Data Protection Principle
- If the disclosure would breach any of the Data Protection Principles.

Monitoring compliance

8.10. To monitor compliance by these third parties with Data Protection laws, we require the third party organisations to enter into an agreement governing the processing of data, security measures to be implemented, and responsibility for breaches in accordance with the terms of the model Data Sharing Agreement set out in Appendix 3.

8.11. Personal data is from time to time shared amongst the organisation and third parties who require to process personal data that we process as well.

8.12. Both the third party and we will be processing that data in our separate capacities as data controllers.

9. Data processors

9.1. A data processor is a third-party entity that processes personal data on our behalf and is frequently engaged if work is outsourced (e.g. payroll, maintenance, and repair works).

9.2. A data processor must comply with Data Protection laws. Data processors must ensure they have appropriate technical security measures in place, maintain records of processing activities and notify us if there is a data breach.

9.3. If a data processor wishes to sub-contract their processing, prior written consent must be obtained from us. Upon a sub-contracting of processing, the data processor will be liable in full for the data protection breaches of their sub-contractors.

9.4. Where we contract with a third party to process personal data, we require the third party to enter into a Data Protection Addendum.

10. Data storage and security

10.1. All personal data we hold must be stored securely, whether electronically or in paper format.

Paper storage

10.2. If personal data is stored on paper it should be kept in a secure place where only authorised personnel can access it.

10.3. Employees should make sure that no personal data is left where unauthorised personnel can access it.

10.4. When the personal data is no longer required it must be disposed of by the employee to ensure its destruction.

10.5. If the personal data requires to be retained on a physical file then the employee should ensure that it is affixed to the file which is then stored following our storage provisions.

Electronic storage

10.6. Personal data stored electronically must also be protected from unauthorised use and access.

10.7. Personal Data should be password protected when being sent internally or externally to data processors or those with whom we have entered into a Data Sharing Agreement.

10.8. If Personal data is stored on removable media (CD, DVD, USB memory stick) then that removable media must be stored securely at all times when not being used. Personal Data should not be saved directly to mobile devices and should be stored on designated drivers and servers.

11. Breaches

11.1. Sometimes a breach of information/data security may occur because personal information has been:

- Accidentally disclosed to an unauthorised person or persons
- Lost, for example, through human error or due to fire or flood or other damage to the premises at which it was held
- Stolen, for example, as a result of a targeted attack (such as a break-in or via cyber-attack) or theft
- Otherwise misused

11.2. A data breach can occur at any point when handling personal data and the organisation has reporting duties in the event of a data breach or potential breach occurring.

11.3. Breaches that pose a risk to the rights and freedoms of the data subjects who are the subject of the breach are required to be reported externally following Section 7.3.

Internal reporting

11.4. We take the security of data very seriously and in the event of a breach will take the following steps:

- As soon as the breach or potential breach has occurred, the DPO must be notified of the breach or potential breach and be provided with all information available about the breach or potential breach.
- We will seek to contain the breach by whatever means available;
- The DPO will consider whether the breach requires to be reported to the Information Commissioner Office (“ICO”) and data subjects affected
- Notify third parties in accordance with the terms of any applicable Data Sharing Agreements

Reporting to the ICO

11.5. The DPO is required to report any breaches which pose a risk to the rights and freedoms of the data subjects who are subject of the breach to the ICO within 72 hours of the breach occurring.

11.6. The DPO must also consider whether it is appropriate to notify those data subjects affected by the breach.

Data Protection Officer ("DPO")

11.7. A Data Protection Officer is an individual who has an over-arching responsibility and oversight over compliance with Data Protection laws.

11.8. We directly employ a Data Protection Officer whose details are noted on the Bield website and contained within the Fair Processing Notice, a sample of which is shown in Appendix 2.

11.9. The DPO is responsible for:

- monitoring compliance with Data Protection laws and this Policy
- co-operating with and serving as Bield's contact for discussions with the ICO
- reporting breaches or suspected breaches to the ICO and data subjects in accordance with Section 10.

12. Individual rights

12.1. We will uphold the rights of data subjects to access and retain control of their data held by us.

Right to be informed

12.2. We will ensure individuals are informed of the reasons for processing their data in a clear, transparent, and easily accessible format informing them of all their rights.

Right to access

12.3. We will ensure that individuals are aware of their right to obtain confirmation that their data is being processed and can access copies of their data and other information.

12.4. Data Subjects are entitled to view the personal data held about them, whether in written or electronic form.

12.5. Data subjects have a right to request a restriction of processing their data, a right to be forgotten, and a right to object to the processing of their data. These rights are notified to tenants and other customers in the Fair Processing Notice.

Right to rectification

12.6. We will correct personal information that is found to inaccurate without undue delay. We will advise data subjects on how to inform us that their data is inaccurate.

Subject access requests

12.7. We will help data subjects view their data we hold when they request to do so (a Subject Access Request).

12.8. Upon receipt of a request by a data subject, we will respond to the Subject Access Request within 30 working days of the date of receipt of the request.

12.9. We must provide the data subject with an electronic or hard copy of the personal data requested unless any exemption to the provision of that data applies in law.

12.10. Where the personal data comprises data relating to other data subjects, we must take reasonable steps to obtain consent from those data subjects to the disclosure of that personal data to the data subject who has made the Subject Access Request.

12.11. Where we do not hold the personal data sought by the data subject, we must confirm this to the data subject as soon as practicably possible, and in any event, no later than one month from the date on which the request was made.

The right to be forgotten/erasure

12.12. We will advise data subjects of their right to request the deletion or removal of personal data where processing is no longer required or justified.

12.13. However, the right to be forgotten is not an absolute right. Where we are legally bound to retain certain information or it has a legitimate interest to retain information, we are entitled to refuse a request to be forgotten.

12.14. Each request received will be considered on its own merits and legal advice may be sought from time to time.

12.15. The DPO will have responsibility for accepting or refusing the data subject's request in accordance with this section and will respond in writing to the request. Where the request is refused, the DPO will explain the rationale of this decision when responding to the requester.

The right to restrict or object to processing

12.16. We will restrict processing when a valid request is received by a data subject and inform individuals of how to exercise this right.

12.17. If direct marketing is undertaken from time to time, a data subject has an absolute right to object to processing of this nature, and if we receive a written request to cease processing for this purpose, then we must do so immediately.

12.18. Each request we receive will be considered on its own merits and legal advice will be sought if required. The DPO will have responsibility for accepting or refusing the data subject's request in accordance with Section 12 and will respond in writing to the request.

Right to data portability

12.19. We will, where possible, allow data to be transferred to similar organisations in a machine-readable format.

13. Privacy by design - data protection impact assessments ("DPIAs")

13.1. We must implement technical and organisational measures to demonstrate that we have considered and integrated data protection into our processing activities throughout the organisation.

13.2. When introducing any new type of processing, particularly using new technologies, we will take into account whether the processing is likely to result in a high risk to the rights and freedoms of individuals and carry out data protection impact assessment.

13.3. 'Data protection impact assessments' are a means of assisting the organisation in identifying and reducing the risks that our operations have on the personal privacy of data subjects.

13.4. We shall:

- Carry out a DPIA before undertaking a project or processing activity that poses a "high risk" to an individual's privacy. High risk can include but is not limited to, activities using information relating to health or race, or the implementation of a new IT system for storing and accessing Personal Data; and

- Include a description of the processing activity, its purpose, an assessment of the need for the processing, a summary of the risks identified and the measures that it will take to reduce those risks, and details of any security measures that require to be taken to protect the personal data
- We will consult the ICO if a DPIA identifies a high level of risk that cannot be reduced.
- The Data Protection Officer ("DPO") will be responsible for such reporting, and where a high level of risk is identified by those carrying out the DPIA they require to notify the DPO within five (5) working days.

14. Archiving, Retention, and Destruction of Data

14.1. We cannot store and retain Personal Data indefinitely. Personal data should only be retained for the period necessary.

14.2. We will ensure that all personal data is archived and destroyed following the Retention Schedule.

15. Publicising and Accessibility

15.1. We will make this policy and associated information available on the Bield website.

15.2. We are happy to translate any of our policies and provide an interpreter if our customers need help.

16. Training and Competence

16.1. All staff will be aware of good practice in data protection and where to find guidance and support for data protection issues.

16.2. Adequate and role-specific training will be provided regularly to everyone who has access to personal data, to ensure they understand their responsibilities when handling data.

16.3. All colleagues are required to undertake training on data protection every three years. Training is offered and recorded on Academy 10.

16.4. Data Protection Audits will be

17. Scheme of Delegation

17.1. As the governing body with responsibility for overseeing our work, our **Board** provides leadership and strategic guidance. It also ensures compliance with our policies and procedures. Concerning data protection, its role is twofold:

- *Ultimate responsibility for ensuring that we meet our legal obligations by reviewing and approving a robust Data Protection Policy*

17.2. The **Chief Executive and Senior Management Team** provide leadership and direction in ways that guide and enable us to perform effectively across all services.

17.3. The Head of Policy and Customer Standards is accountable to the Senior Management Team and Performance and Audit Committee for data protection.

17.4. The **Data Protection Officer within the Policy and Customer Standards Team has operational responsibility for monitoring and assisting with the implementation for monitoring and assisting the implementation of the requirements of the Data Protection Act, including**

- Providing advice and support to all employees on all matters relating to compliance with the Data Protection Act
- Disseminating information relating to the Data Protection Act
- Maintaining a register containing all requests, breaches, and enquiries made in relation to the Data Protection Act
- Assisting where required with responding to such requests from individuals to access personal information held about them (subject access request)
- Liaising with the Information Commissioner's Office (ICO) which regulates data protection

17.5. The **Leadership Team** is responsible for monitoring the policy ensuring compliance with the procedures.

17.6. All **colleagues** have a responsibility for ensuring personal data is collected, stored, and handled appropriately and must ensure that it is handled in line with this policy and the data protection principles.

18. Monitoring, Reporting, and Review

18.1. We will review this policy on a five-year basis.

18.2. An annual report will be put to the Board about the previous year, stating any breaches, subject access requests, or DP Impact assessments done.

18.3. We will monitor compliance with the policy by recording and reporting on the following annually:

- Number of data breaches
- Cause of data breaches
- Number of subject access requests

19. Complying with the Law and Good Practice

19.1. It is a legal requirement that we process data correctly. This includes collecting, handling, and storing personal information in accordance with relevant legislation and regulations:

- UK General Data Protection Regulation (UK GDPR)
  Regulation that governs data processing in the United Kingdom.

- Privacy and Electronic Communications Regulations (PECR)
  Gives people specific privacy rights concerning electronic communications.

- Data Protection Act 2018
  Governs how we can obtain, store, share, and use personal data. Specifically, this Act
  - Prevents people or organisations from holding and using inaccurate information on individuals. This applies to information regarding both private lives and business.
  - Gives the public confidence about how business' can use their personal information.
  - Provides data subjects with the legal right to check the information businesses hold about them. They can also request for the data controller to destroy it.
  - Gives data subjects greater control over how data controllers handle their data.
  - Emphasises accountability. This requires businesses to have processes in place that demonstrate how they're securely handling data.
  - Requires firms to keep people's data safe and secure. Data controllers must ensure that it is not misused.
  - Requires the data user or holder to register with the Information Commissioner.

- Human Rights Act 1998

- Regulation of Investigatory Powers (Scotland) Act 2000
- Crime and Disorder Act 1998
- Freedom of Information (Scotland) Act2002
- Environmental Information (Scotland) Regulations 2004
- Management of Offenders etc (Scotland) Act 2005
- Antisocial Behaviour etc (Scotland) Act 2004
- Police Act 1997
- Serious Organised Crime and Police Act 2005
- Information Commissioner's Office Data Protection Code: Employment Practices
- Information Commissioner's Office Data Protection Code: Subject Access Request;
- Information Commissioner's Office Code of Practice: Data Sharing
- Information Commissioner's Office Code of Practice: Consent; and
- all other relevant guidance and Codes of Practice published by the Information Commissioner's Office from time to timer

19.2. As a Registered Social Landlord (RSL), we are regulated by the Scottish Housing Regulator (SHR). The SHR's statutory objective is to safeguard and promote the interests of current and future tenants, homeless people, and other people who use services provided by social landlords. In developing our policy, we have taken account of good practice, including that developed by the Scottish Housing Regulator.

19.3. The SHR uses the outcomes and standards in the Charter to assess the performance of social landlords. The key outcomes that have been considered in the development of this policy are

Outcome 1 Customers have their individual needs recognised, are treated fairly and with respect, and receive fair access to housing and housing services.

19.4. As a provider of care, we are regulated by the Care Inspectorate. The Care Inspectorate uses Health and Social Care Standards to assess the performance of care providers. The key standards that have been considered in the development of this policy are:

Standard 4 I have confidence in the organisation providing my care and support

20. GDPR

20.1. We will treat all personal data in line with our obligations under the current data protection regulations and our Privacy Policy. Information regarding how all data will be used and the basis for processing your data is provided in our Customer Fair Processing Notice.

21. Sustainability statement

21.1. We will endeavour to work in a way that minimises the use of resources.

22. Risk management

22.1. Several risk management activities have been identified to ensure this policy is adhered to and that Bield customers experience the best possible experience

- Bield colleagues, Board members, and volunteers are made aware of this policy on publication and during induction of new colleagues.
- Customers and carers are made aware of this policy during service entry.

Appendix 1 Equality Impact Assessment

1	**Title of Policy to be assessed**: Data Protection Policy
2	**Date: 16/11/2021**
3	**Lead Officer/Manager: Zhan McIntyre**
4	**EQIA Team (who will be involved): N/A**
5	**Director/Manager: Tracey Howatt**
6	**Is the function or policy existing, new, or review: Review**
7	**Set out the aims/objectives/purposes/outcomes of the function or policy, and give a summary of the service provided:** The purpose of this policy is to ensure that we manage personal data and information in line with relevant legislation. **The policy applies to all Bield colleagues**
7a	**Who should benefit from the policy (target population): All customers**
7b	**Linked policies, functions: Are there any other functions, policies or services, which might be linked with this one for this exercise? Please list.**
8	**State whether the policy will have a positive or negative impact across the following factors and provide initial comments/observations.**
	Age: Older people, people in the middle years, young people, and children. **Disability:** includes physical disability, learning disability, sensory impairment, long-term medical conditions, mental health problems. **Maternity and civil partnership** **The policy will have no impact on people expecting or recently giving birth or within a civil partnership** **Race:** Minority ethnic people (includes Gypsy/Travellers, non-English speakers). **Religion or belief:** includes people with no religion or belief. **Sex:** Women, men, and transgender people (include issues relating to pregnancy and maternity). **Gender reassignment:** The process of changing or transitioning from one gender to another. **Sexual orientation:** Lesbian, gay, bisexual, and heterosexual people. **People in remote, rural, and/or island locations** **People in different work patterns:** e.g. part-/full-time, short-term, job share, seasonal **People who have low literacy** **People in different socio-economic groups** (includes those living in poverty/people on a low income)

	Population groups	Positive Impact	Negative Impact	Comments
	Age	**N/A**	**N/A**	**Large print available**
	Disability	**N/A**	**N/A**	Easy read version available
	Maternity and civil partnership	**N/A**	**N/A**	
	Race	**N/A**	**N/A**	Translation message on the back cover.
	Religion or belief	**N/A**	**N/A**	
	Sex and Gender reassignment	**N/A**	**N/A**	
	Sexual orientation	**N/A**	**N/A**	
	People in remote, rural, and/or island locations	**N/A**	**N/A**	
	People in different work patterns	**N/A**	**N/A**	
	People who have low literacy	**N/A**	**N/A**	
	People in different socio-economic groups	**N/A**	**N/A**	
9	**What evidence do you have for the statements you have made above? Focus on:** • Needs and experiences; • Uptake of services; N/A • Levels of participation. N/A			
10	**From the evidence set out what actions, if any, will you take where the negative impact has been identified:**			

Population groups	Proposed action	How will it address the negative impact?
Age	**Large print version**	**Information available in an accessible format**
Disability:	**Easy read version**	**Information available in an accessible format**
Maternity and civil partnership	**N/A**	**N/A**
Race	**Translate to common languages including:** **Polish** **Lithuanian**	**Information available in an accessible format**
Religion or belief	**N/A**	**N/A**
Sex and Gender reassignment	**N/A**	**N/A**
Sexual orientation	**N/A**	**N/A**

People in remote, rural, and/or island locations	**N/A**	**N/A**
People in different work patterns	**N/A**	**N/A**
People who have low literacy	**N/A**	**N/A**
People in different socio-economic groups	**N/A**	**N/A**

Briefly explain how the policy contributes to our equality and diversity values by answering the following questions:

- How will it provide equality of access to services, information, and employment?
- Does it or could it celebrate diversity?
- Will it or could it promote good relationships within and between communities?
- How will it provide good quality, inclusive services?

N/A

Any additional information, questions, or actions required? Please explain.

Sign off:
As Director I am satisfied with the results of this EIA
The findings will be referred to within Service Plans and target set. The Action Plan will be reviewed annually within Business planning reporting.

Signature: **Date:**

Appendix 2 Sample fair processing notice

Vision, mission, and values

Our vision is a Scotland where people of all ages are respected can make their own choices, and lead independent and fulfilling lives.

Our mission is to improve the quality of life of older people by offering a diverse range of housing, care, and other services.

Our values are

Honesty	Equality and Diversity
Ambition	Dignity
Integrity	Caring
Kindness	

This notice explains what information we collect when we collect it and how we use this.

During our activities, we will process personal data (which may be held on paper, electronically, or otherwise) about you and recognise the need to treat it appropriately and lawfully.

The purpose of this notice is to make you aware of how we will handle your information.

Who are we?

Bield Housing & Care (Scottish Charity Number SC006878) is a registered society under the Co-operative and Community Benefit Societies Act 2014 with Registered Number 1692R (S) and have our Registered Office at 79 Hopetoun Street, Edinburgh, EH7 4QF.

We are notified as a 'Data Controller' with the Information Commissioner's Office under registration number Z5643453, and we are the data controller for any personal information you provide us.

Information that we hold and how we use it

We collect information about you:

- When you apply for housing with us, become a tenant, request services (e.g. care services or repairs), enter into a factoring agreement with ourselves howsoever arising, or otherwise provide us with your details
- If you are a BR24 customer, calls will be recorded for quality control, training, and to protect staff and service users
- When you apply to become a member of Bield Housing & Care or Board member of Bield Housing & Care or sub-committees
- From your use of our online services e.g. applying for housing, reporting any tenancy/factor related issues, making a complaint
- From your arrangements to make payment to us (such as bank details, payment card numbers, employment details, benefit entitlement, and any other income and expenditure-related information).
- From members of your household or other representatives, for example, a person with written authorisation from you to act on your behalf or a person awarded power of attorney/Guardianship.

We may collect the following information about you:

- ✓ Name
- ✓ Address
- ✓ Gender
- ✓ Ethnicity
- ✓ Date of birth
- ✓ Telephone number
- ✓ Email address
- ✓ National insurance number
- ✓ Next of kin and emergency contacts
- ✓ Power of Attorney
- ✓ Disability details
- ✓ Health, wellbeing, and support details
- ✓ Housing benefits reference number
- ✓ Identifiable imagery eg CCTV images, photographs for file plans
- ✓ Bank account details

We may also collect and store your demographic information, such as gender, race or ethnic origin, age, date of birth, marital status, nationality, education/work histories, employment details.

We receive the following information from third parties:

- Benefits information, including awards of Housing Benefit/ Universal Credit
- Health professionals such as GPs
- social services or the police, banks, and mortgage providers
- Payments made by you to us
- Complaints or other communications regarding behaviour or other alleged breaches of the terms of your contract with us, including information obtained from Police Scotland
- If you are a tenant - reports as to the conduct or condition of your tenancy, including references from previous tenancies, and complaints of anti-social behaviour
- If you require a medical adaptation – your personal details, confirmation of eligibility, and reasons for adaptation
- Other agencies working with you to whom you have given consent

Why we collect this information and how it will be used:

- To undertake and perform our obligations and duties to you in accordance with the terms of our contract
- To enable us to supply you with the services and information as requested
- To enable us to respond to your repair request, application for housing or care services, and complaints
- To analyse the information we collect so that we can administer, support and improve and develop our business and the services we offer
- To contact you to provide details of any changes to our suppliers or services which may affect you
- For all other purposes consistent with the proper performance of our operations and business
- To contact you for your views on our products and services.

Sharing of your information

The information you provide to us will be treated by us as confidential.

We may disclose your information to other third parties who act for us for the purposes set out in this notice or for purposes approved by you, including the following:

- If we enter into a joint venture with or merged with another business entity, your information may be disclosed to our new business partners or owners
- If we instruct repair or maintenance works or medical adaptations, your information may be disclosed to any contractor
- If we are investigating a complaint, information may be disclosed to Police Scotland, Local Authority departments, Scottish Fire & Rescue Service, and others involved in any complaint, whether investigating the complaint or otherwise
- If we are updating tenancy details, your information may be disclosed to third parties (such as utility companies and Local Authority)
- If we are investigating payments made or otherwise, your information may be disclosed to payment processors, Local Authority and the Department of Work & Pensions
- If we are obliged to provide your personal information regulation e.g. the Care Inspectorate
- Your details may be shared with National TV Licensing Authority
- In the event of an emergency, your details may be shared with an emergency service, NHS, care, and support services
- We may share your details with our solicitors and auditors
- If we are conducting a survey of our products and/or service, your information may be disclosed to third parties assisting in the compilation and analysis of the survey results
- Other agencies working with you to whom you have given consent.

Unless required to do so by law, we will not otherwise share, sell or distribute any information you provide to us without your consent.

Transfers outside the UK and Europe

Your information will only be stored within the UK and EEA.

Security

When you give us information we take steps to make sure that your personal information is kept secure and safe following Bield Housing & Care Data Protection Policy.

All of our systems are password protected and all paper copies are stored in locked cabinets.

How long we will keep your information

We review our data retention periods regularly and will only hold your personal information for as long as is necessary for the relevant activity, or as required by law (we may be legally required to hold some types of information), or as set out in any relevant contract we have with you.

Your Rights

You have the right at any time to:

- ask for a copy of all personal information we hold on you
- request we correct any inaccuracies in your personal information
- request us to delete your personal information
- object to receiving any marketing communications from us.

If you would like to exercise any of your rights above or have any queries regarding our data protection practices, please contact our Data Protection Officer, Chrisleen Schutte, on 0131 273 4000 or email dataprotection@bield.co.uk

If you are unhappy with how we handle your personal information, you have the right to complain to the Information Commissioner's Office.

Their details are:

The Information Commissioner's Office – Scotland 45 Melville Street, Edinburgh, EH3 7HL Telephone: 0303 123 1115 Email: Scotland@ico.org.uk

The accuracy of your information is important to us

Please help us keep our records updated by informing us of any changes to your email address and other contact details.

Appendix 3 Key considerations for sharing information

(A) Systematic Sharing

- ☐ Is the sharing justified?
- ☐ What is the sharing meant to achieve?
- ☐ Have the potential benefits and risks to individuals whose personal information is involved been assessed?
- ☐ Is the sharing proportionate to the issue you are addressing?
- ☐ Could the objectives be achieved without sharing personal information?
- ☐ Has the information been given to us in confidence?
- ☐ Is there any requirement for consent to be given before such personal information can be shared (and, if so, is that consent in place)?
- ☐ Is there any legal obligation to share personal information?

(B) One-off request

- ☐ Is the sharing justified?
- ☐ Have the potential benefits and risks to those individual(s) whose information is involved been assessed?
- ☐ Are there concerns that the individual(s) whose personal information is involved is at risk of serious harm?
- ☐ Has the information been given to the Group in confidence?
- ☐ Is there any requirement for consent to be given before such personal information can be shared (and, if so, is that consent in place)?
- ☐ Is there any legal obligation to share personal information?

If the decision is taken to share personal information in these circumstances, key points to additionally consider include:

- ☐ Has the identity of the person requesting the information been validated? This is essential. •
- ☐ Is it clear what personal information has been requested?
- ☐ What personal information needs to be shared? Only share what is necessary.
- ☐ How should personal information be shared?
- ☐ Personal Information must be shared securely.
- ☐ Is it appropriate/safe to inform the individual that their personal information has been shared?
- ☐ Do other privacy laws apply?
- ☐ Are there any other legal obligations or rules other than the Data Protection Legislation which may apply to the sharing, for example, contractual duties, duties of confidence, industry-specific regulation, or copyright?
- ☐ How will the parties provide individuals with the personal information they are entitled to regarding the Processing for transparency and fairness?

If the decision is taken to share personal information, a data-sharing agreement should be put in place to set out the parameters of the agreement and to underpin the arrangements for the sharing, before any personal information is shared within another party.

A data-sharing agreement should cover:

- ☐ What information needs to be shared – detailed datasets
- ☐ The organisations that will be involved
- ☐ The purpose(s) of the information-sharing exercise and the period during which the sharing exercise will operate
- ☐ A statement explaining why the sharing is proportionate to the purpose(s)
- ☐ Obligations to ensure that the information is accurate and provisions for recording in the same format

☐ Measures to ensure adequate security measures are implemented and maintained to protect the information
☐ Agreed technical and organisational security arrangements for the transmission of information
☐ What arrangements need to be in place to provide individuals with access to their personal information, and deal with any other requests from individuals and complaints
☐ Agreed common retention periods for holding the information
☐ Procedures for dealing with breaches
☐ Processes to ensure the secure deletion of the information take place; and
☐ Provisions for reviewing and terminating the agreement.

Once a decision has been made as to whether or not information should be shared, that decision must be recorded, together with the reasoning behind that decision. Where a decision was taken to share the information, an audit trail must be kept to include details of the following

What personal information was shared and for what purpose(s)
☐ Whom it was shared with
☐ When it is shared
☐ The justification for sharing
☐ Whether the personal information was shared with or without the consent of the individual
☐ Whether a data-sharing agreement was put in place for the sharing exercise (and if not, the reasoning as to why not).

Transferring personal information outside the EU
When sharing personal information that we are the controller of, we must consider whether this will result in any personal information being transferred outside the EU.

For example, many cloud-based servers are located within the United States, and transferring personal information to an organisation that will store it on a server located in the US will result in a transfer outside the EU.

We must also be aware of sharing any personal information with international organisations to ensure that the requirements of the GDPR are met. The Group should only transfer personal information outside the EU or to an international organisation in the following circumstances:

1. The European Commission has decided that the country or international organisation ensures an adequate level of protection and issues an 'adequacy notice' under the GDPR;
2. If transferring to the US, whether the personal information transfer is covered by the EU-US Privacy Shield framework
3. Where we have put in place appropriate safeguards and there are enforceable rights and effective legal remedies for individuals; or
4. One of the derogations under the GDPR applies.

Appropriate safeguards will apply where:
- there is a legally binding and enforceable instrument between public authorities or bodies
- the ICO has approved binding corporate rules under the GDPR
- the standard data protection clauses as adopted by the European Commission or by the ICO and approved by the European Commission are put in place
- there is an approved code of conduct or certification mechanism in place in accordance with the terms of the GDPR.

The derogations in the GDPR provide that personal data may be transferred outside the EU for certain specific situations where:

- the individual has consented to the transfer
- the transfer is necessary for the performance of a contract between us and the individual, including pre-contractual steps requested by the individual, or a contract made in the interests of the individual between us and another person
- the transfer is necessary for important reasons of public interest;
- the transfer is necessary to establish, exercise, or defend legal claims;
- the transfer is necessary to protect the vital interests of the individual or other persons, where the individual is physically or legally incapable of giving consent; or
- the transfer is made from a register, which under UK or EU law is intended to provide information to the public.

Speaking your language - we are happy to translate our policies on request.

يمكن ترجمة سياساتنا عند الطلب.
إذا كنت بحاجة إلى مساعدة ، فيمكننا توفير مترجم

Nasze zasady mogą być przetłumaczone na żądanie.
Jeśli potrzebujesz pomocy, możemy zapewnić tłumacza

我们的政策可以应要求翻译。
如果您需要帮助，我们可以提供翻译

ہماری پالیسی کا درخواست پر ترجمہ کیا جاسکتا ہے۔
اگر آپ کو مدد کی ضرورت ہو تو ہم ایک ترجمان فراہم کرسکتے ہیں