Acceptable Use Policy

BIELD
FREE TO BE

Title of Policy	Acceptable Use Policy
Approved by	
Approval Date	04/02/2026
Owner	Director of People and OD
Author	Head of Technology
Version	V01
Period of Review	
Date of Review	01/02/2029
Lead Directorate	People and OD
Stakeholders	☐ Partnership Forum ☒ Human Resources ☒ ICT ☒ Staff Forum ☒ Property ☐ Other ☒ Finance ☒ BR24 ☒ Assurance and Business Planning ☒ Operations ☒ Assets
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 Technology underpins our Independent Living Approach – enabling staff to work efficiently, connect meaningfully with tenants, and deliver services in a person-centred, respectful and secure way.

1.4 This Technology Acceptable Use Policy sets out standards and expectations for the responsible, secure and ethical use of Bield digital systems. It ensures technology is used to empower colleagues, enhance service delivery, and promote tenant autonomy, privacy and digital inclusion.

1.5 This policy embodies our values, which are:

Honesty	Equality and Diversity	Ambition	
Dignity	Integrity	Caring	Kindness

2 Purpose

2.1 The purpose of this policy is to ensure that all Bield employees, contractors, and third-party providers use Bield's digital systems in a way that is:

- Safe, secure and lawful
- Aligned with Bield's values and regulatory requirements
- Supportive of our Independent Living Approach
- Consistent with our commitment to dignity, respect and safeguarding of tenants, staff and the wider public

2.2 This policy aims to:

- Safeguard the security, integrity, and availability of Bield's IT systems and resources
- Protect sensitive data, intellectual property, and organisational reputation
- Promote responsible, transparent user behaviour by clarifying expectations, roles, and consequences of misuse
- Ensure compliance with relevant legislation and best practice, including data protection and cyber security obligations

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 in relation to this policy, and this is included at Appendix 1

3.2 In line with our Independent Living Approach and commitment to inclusive service delivery, the following measures will be taken to ensure this policy is accessible and understandable to all:

- A large print version is available
- Translation and interpretation message on the back of the policy
- Easy to read version for users with a cognitive impairment or learning differences

4 Scope

4.1 The policy applies to all Bield-provided IT systems and resources, including, but not limited to:

- Desktop computers and laptops
- Tablets and smartphones
- Printers and scanners
- Internet of Things (IoT), including smart technology, digital assistants and similar devices
- Software applications and platforms
- Email, internet, and intranet
- Social media accounts used in a professional capacity
- Cloud-based services and collaboration tools

4.2 The policy also applies to the use of personal devices or accounts when used for work-related activities, including, but not limited to:

- Accessing Bield's network, systems, or email
- Using messaging platforms or for work communication
- Publishing or interacting on social media were representing or referencing Bield in any capacity

4.3 The policy covers all individuals who interact with Bield's digital systems in a professional or work-related capacity, including:

- Employees and casual workers
- Volunteers and board members
- Contractors, consultants, agency workers, and other third parties delivering services on behalf of Bield

4.4 The policy supports the safe and effective use of technology to deliver services aligned with Bield's Independent Living Approach, where digital tools are enablers of tenant autonomy, staff efficiency, and secure, respectful communication

5 Policy Principles

5.1 The following principles apply to all users of Bield's IT systems and digital resources. All users must:

- Comply with all applicable laws, regulations, and Bield's internal policies, procedures and training when using IT resources and systems
- Respect privacy by refraining from unauthorised access to, or manipulation of, data. This includes not accessing, copying, modifying, deleting or sharing data unless explicitly authorised
- Protect Bield data and information by using strong passwords and multi-factor authentication (MFA), and reporting any actual or suspected data security breaches (see Appendix 2 for more details)
- Use IT resources efficiently and responsibly, minimising personal use and avoiding activity that is excessive, disruptive, or contrary to Bield's values
- Protect Bield's reputation, and avoid actions that could damage Bield's reputation, data security, or expose it to risk
- Request additional access through the IT Service Desk where required
- Report any suspected or actual data incident or breaches to ICT Service Desk, Data Protection Officer or line manager

- Accept that Bield may monitor or restrict access in line with its legal responsibilities and disciplinary procedures

5.2 Bield reserves the right to monitor, audit and review the use of IT resources and systems by users, in accordance with legislation and internal policies and procedures. Access may be suspended, restricted, or withdrawn where misuse is identified or suspected

5.3 Breaches of this policy will be addressed in accordance with Bield's Disciplinary and Dismissal Procedure. For third parties, relevant contractual or procedural mechanisms will apply. Where appropriate, Bield may report breaches to regulatory bodies or law enforcement

5.4 The recording of Teams, Zoom or any other form of online meetings is only permitted with the informed, explicit consent of all parties in advance. Recording should not be considered routine practice. Consent may be secured via email invitations or verbal communication confirmation at the outset. Covert or unauthorised recording undermines trust and is strictly prohibited. Any recordings must be stored and retained in line with GDPR requirements and Bield's Data Protection Policies and Procedures

Acceptable Use

5.5 Acceptable use refers to using IT and other digital systems to support your work tasks efficiently and effectively

5.6 This includes safeguarding login credentials (e.g. passwords), using approved tools, and handling sensitive data only in appropriate environments. For instance, accessing confidential data within a secure office setting is acceptable, whereas doing so in a public space is not.

Unacceptable use of IT

5.7 Unacceptable use of IT comprises any actions that:

- Disrupt work productivity
- Compromise Bield's, our tenants', customers' or partners' data security
- Breach laws or organisational policies
- Fail to consider contextual risk

5.8 Examples include, but are not limited to:

- Sharing (deliberately or accidentally) login credentials (if passwords) with unauthorised persons
- Accessing systems or data without appropriate permissions
- Storing sensitive data insecurely (i.e. it could easily be lost or stolen)
- Using unapproved tools or processes to store sensitive information, such as passwords or credit card details
- Using your work email address for personal tasks
- Excessive personal use during working time
- Installing unauthorised software
- Forwarding Bield's data to your personal devices or accounts
- Using work email for personal tasks
- Using a computer that is logged in under someone else's details
- Unauthorised removal of Bield technology from a Bield site

Clear desk policy

5.9 Bield operates a clear desk policy to reduce the risk of data breaches. Staff must:

- Log off from applications and/or network services when not in use

- Lock workstations, laptops and smartphones when unattended
- Secure confidential materials in locked storage when away from the workplace or at the end of the day

Email and Messaging

5.10 Bield's email and messaging systems are for business use. The following is not permitted:

- Using email for personal gain
- Sending or knowingly receiving obscene, defamatory, or harassing content
- Presenting personal opinions as those of Bield
- Transmitting copyrighted or unauthorised materials
- Sharing confidential, financial, or property information inappropriately
- Work related emails should not be forwarded to personal accounts

5.11 Care must be exercised when corresponding with personal email addresses of third parties. In particular, be wary of emails from personal email addresses (gmail.com etc) that purport to be from businesses

5.12 Do not click suspicious links or open unexpected attachments Immediately notify the IT Service Desk of any suspicious or unexpected attachments or digital communications.

Internet

5.13 Confidential information must not be transmitted online without ensuring data security and recipient identity

5.14 Unauthorised internet activity includes:

- Playing recreational games
- Gambling
- Streaming non-work-related media
- Accessing personal social media
- Viewing or distributing inappropriate content
- Attempting unauthorised network access
- Breaching any other Bield policies
    - Remote users must comply with the same internet use policies as office-based staff

Mobile devices and bring your own device (BYOD)

5.15 Personal devices are not permitted to connect to the corporate network

5.16 Bield will supply suitable devices for work. Any issues must be referred to this IT service desk

5.17 Smartphones are configured with separate Personal and Work profiles. Data cannot be copied or moved between the two profiles The Bield Technology Team may remotely wipe the Work profile in the event of loss or breach

5.18 Devices must run on the most current supported operating system

5.19 Bield provide a Guest Wi-Fi system at offices and most developments. This can be used by personally owned devices and by Bield supplied devices when accessing cloud services such as Microsoft 365

Physical Security

5.20 Devices and workstations must be locked, or logged out of, if the user is leaving the immediate area. This is to ensure that no one else can access the user's information or can use the workstation without identifying themselves. In addition, users must: Prevent others from viewing screens with confidential information

- Safeguard Bield supplied devices from theft or damage
- Encrypt data stored on portable devices using approved Bield supplied software
- Refrain from using recording devices in secured areas
- Display photo ID while in the building
- Badge in/out of secure areas and avoid tailgating or door propping
- Escort visitors in secure areas at all times
- Avoid eating/drinking in server rooms and take care near devices

Incidental Personal Use

5.21 As a convenience to Bield employees, occasional personal use of Information Resources is permitted. The following restrictions apply:

- Incidental personal use of electronic communications, Internet access, printers, copiers, and so on, is restricted to Bield employees; it does not extend to family members or other acquaintances
- Incidental use should not result in direct costs to Bield and must not inconvenience or distract other business activities
- Incidental use should not interfere with the normal performance of an employee's work duties.
- It must not impede the work of others
- It must not make excessive use of Bield IT Resources (i.e. prevent others accessing technology or systems)
- No files or documents may be sent or received that may cause legal action against, or embarrassment to, Bield, its staff or its customers

Sanctions

5.22 Failure to comply with this policy and subsidiary policies, procedures or regulations, may result in withdrawal of access to Bield's IT and digital services and may result in disciplinary action, including dismissal for employees or termination of contract for agency staff, contractors or other third parties

Exceptions

5.23 If an individual or third party cannot comply with this policy, they must contact the IT Service Desk for advice on how to enable compliance, otherwise they must cease using Bield's data and IT services

6 Publicising and Accessibility

6.1 This policy, along with relevant supporting information, will be published on the Bield website and included in the Employee Handbook to ensure it is accessible to staff, volunteers, Board members and the wider public

6.2 Bield is committed to promoting inclusive access. We will provide translations of this policy and arrange interpreter support upon request to ensure that all customers and staff can understand and engage in the contents

7 Training and Competence

Security Training and Awareness

7.1 All new employees must complete mandatory security awareness training course(s) within 90 days of being granted access to any information resources

7.2 Employees must be provided with and acknowledge they have received and agree to adhere to the Information Security Policies before they are granted to access to information resources

7.3 All employees must complete annual security awareness training to maintain their knowledge of current information security practices and responsibilities

8 Scheme of Delegation

Board responsibilities

8..1 As the governing body, the Board provides strategic leadership and oversight of Bield's operations. In relation to the Acceptable Use Policy, the Board is responsible for:

- *Approving the strategic framework*

Chief Executive responsibilities

8.2 The Chief Executive provides overall leadership and strategic direction, ensuring that effective policies and procedures are in place. This includes ensuring the implementation and continued relevance of the policy in ways that guide and enable us to perform effectively across all services. This includes approving the acceptable use policy

Head of IT responsibilities

8.3 Responsible for the implementation, monitoring and periodic review of the Acceptable Use Policy including:

- Ensuring technical controls are in place to support compliance
- Monitoring system usage and responding to security incidents
- Providing guidance and support to staff on acceptable use

Line Managers responsibilities

8.4 Line managers are responding for:

- Ensuring that staff under their supervision understand and adhere to this policy
- Escalate non-compliance or concerns in line with internal procedures

All staff

8.5 All Bield employees must:

- Read, understand, and comply with the Acceptable Use Policy and related information security policies
- Complete required training and report any breaches or risks promptly

8.6 All **colleagues** should be aware of:

- Information Security Policy
- Email Policy
- Password Policy
- Data Protection Policy

- Data Protection Act 2018
- Freedom of Information Policy
- Managing Information Securely

9 Monitoring, Reporting, and Review

9.1 The policy shall be updated regularly to remain current in the light of any relevant changes to any applicable law, Bield's policies or contractual obligations and reviewed by the Digital Governance Group at least every three years.

9.2 Minor reviews of this policy will be undertaken by the Head of IT as required and will be approved by the Digital Governance Group

10 Complying with the Law and Good Practice

10.1 In developing this policy, we have taken into account the following internal policies, legal frameworks and external standards and guidance:

Internal Bield policies and frameworks

- Bield Network Monitoring and Patching Policy
- Bield Firewall Policy
- Bield Privileged Access Policy
- Bield Backup and Disaster Recovery Policy
- Bield Cyber Incident Response Policy
- Bield Data Classification Policy
- Bield Risk Management Policy
- Bield Data Protection Policy
- Bield Freedom of Information Policy
- Bield Retention Schedule
- Bield Records Management Policy

Legislation and regulatory requirements

- Data Protection Act 2018
- Data Privacy Impact Assessment
- Information commissioner's office - GDPR Guidance

Industry standards and best practice

- ISO/IEC 27001:2022 - Information Security Management Systems
- PCI DSS - Payment Card Industry Data Security Standard
- National Cyber Security Centre – Cloud Security Principals
- National Cyber Security Centre - Cyber Essentials Guidance

Scottish Housing Regulator

10.2 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 take account of good practice including that developed by the Scottish Housing Regulator

10.3 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 13	Customers receive services of continually improving value for rent and other charges they pay.
Outcome 14	We strike a balance between the level of service provided the cost of services and how far current and prospective customers can afford them.

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: [delete as appropriate]

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

11 GDPR

11.1 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

12 Risk Management

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**: Acceptable Use Policy
2	**Date:** 19/02/2025
3	**Lead Officer/Manager**: John Malone
4	**EQIA Team (who will be involved):**
5	**Director/Manager:** Nicola Ritchie
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 outline the acceptable use of IT resources and systems by staff, volunteers and Board members of the Bield Housing and Care. It aims to ensure that IT resources and systems are used in a responsible, secure and lawful manner, and that Bield's data and reputation are protected. **The policy applies to all Bield staff, volunteers and Board of Bield Housing and Care**
7a	**Who should benefit from the policy (target population):** The policy applies universally to all Bield employees, volunteers, and Board members. It specifically provides clear guidance on ICT equipment use both within office premises and for staff engaged in home working.
7b	**Linked policies, functions: Are there any other functions, policies or services, which might be linked with this one for this exercise? Please list.** • Information Security Policy • Email Policy • Password Policy • Data Protection Policy • Data Protection Act 2018 • Freedom of Information Policy • GDPR • All services who use ICT equipment, both in office, development and those staff who work from home
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. Some people in middle years may require additional support with ICT Equipment when they are not familiar when updated ICT equipment is provided by Bield and may require additional training. **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 Staff who have reduced hours may require additional time to complete mandatory training for ICT resources **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	**X**		**Some mid-career staff may require additional ICT training when new systems or updates are developed.**
	Disability	**N/A**	**N/A**	No direct negative impact identified, training accessibility to be ensured for all disabilities.
	Maternity and civil partnership	N/A	N/A	No anticipated impact
	Race	N/A	N/A	No anticipated impact: policy translation and interpreter services available as required.
	Religion or belief	N/A	N/A	No anticipated impact
	Sex and Gender reassignment	N/A	N/A	No anticipated impact
	Sexual orientation	N/A	N/A	No anticipated impacted
	People in remote, rural, and/or island locations	N/A	N/A	No anticipated impact: remote working provisions considered.
	People in different work patterns	X		People with reduced hours may need additional

				time for mandatory ICT training completion.
	People who have low literacy	X		Consideration needed for accessible training materials
	People in different socio-economic groups	N/A	N/A	No anticipated impact
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	**Provide additional tailored ICT training and support**	**Facilitates familiarity and confidence in updated ICT systems.**
Disability:		
Maternity and civil partnership	**N/A**	**N/A**
Race	**N/A**	**N/A**
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	**Allow flexible scheduling for mandatory training completion**	**Ensures all staff can meet training requirements within their work patter**
People who have low literacy	**Develop accessible, plain language training materials**	**Enhances understanding and compliance with policy requirements.**
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: J Malone** **Date: 4 February 2026**

Appendix 2 Password requirements and security

Password requirements differ per system but the general rule is the longer the password the stronger it is. The minimum length of passwords for Windows systems is 12 but we encourage longer passwords by using three or more words completely unconnected to the use or themselves.

If at any time a user believes their password may have been compromised, they must immediately change it or request that it is changed by contacting the ICT service Desk.

Bield have implemented multi-factor authentication or single-sign-on for some systems and these methods should not be bypassed as they provide significant enhancement to our security.

Users must report any actual or suspected breaches of this policy, or any incidents or issues affecting IT resources and systems, to the Head of Technology or the Data Protection Officer as soon as possible.

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