Belmont House, 57 Belmont Road, Cambuslang, G72 8PG
www.wwhc.org.uk E: enquiries@wwhc.org.uk T: 0141 641 8628

Policy Name	**Data Breach Management Procedure**
Policy Author	**DPO / Corporate Services Officer**
Approved by Sub Committee	**N/A**
Approved by Management Committee	**March 2026**
Latest date of Next Review	**March 2029**

West Whitlawburn Housing Co-operative will provide this policy on request at no cost, in larger print, in Braille, in audio or other non-written format, and in a variety of languages. Please contact the office.

Registered with the Scottish Housing Regulator No. 203
Registered Charity No. SCO38737, VAT Registration No. 180223636
Registered society under the Co-operative and Community Benefit Societies Act 2014

1 Introduction

1.1 This Procedure:

1.1.1 places obligations on staff to report actual or suspected personal data breaches; and

1.1.2 sets out our procedure for managing and recording actual or suspected personal data breaches.

1.2 This Procedure applies to all staff, and to all personal data and special category data held by us.

2 Definitions:

For the purposes of this Procedure:

Data Breach Team	means the members of staff at the organisation responsible for investigating personal data breaches;
data subject	means an individual to whom the personal data relates;
personal data breach	means 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;
personal data	means information relating to an individual, who can be identified (directly or indirectly) from that information;
processing	means obtaining, recording, organising, storing, amending, retrieving, disclosing and / or destroying personal data, or using or doing anything with it; and
special category data	means personal data about an individual's race, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership (or non-membership), genetic information, biometric information (where used to identify an individual) and information

concerning an individual's health, sex life or sexual orientation.

3 Responsibility

The Data Protection Officer (DPO) has overall responsibility for this Procedure and for ensuring all staff comply with it.

4 Our Duties

4.1 We process personal data about a number of categories of data subjects, including housing applicants, our tenants (and their household members), job applicants, current and former employees, contractors, business contacts (including at other registered social landlords, regulators, local authorities and agencies), complainants, elected members, apprentices, committee members, and shareholding members for a number of specific lawful purposes relevant to our activities and functions as a registered social landlord in Scotland. As the controller of personal data, we have a responsibility under data protection legislation to protect the security of the personal data that we process about data subjects.

4.2 We must keep personal data secure against loss or misuse. All staff are required to comply with this Procedure.

5 What Can Cause a Personal Data Breach?

A personal data breach can happen for several reasons:

5.1 loss or theft of equipment on which personal data is stored (e.g. loss of a laptop or a paper file)

5.2 inappropriate access controls allowing unauthorised use of personal data

5.3 equipment failure on which personal data is stored

5.4 human error (e.g. sending an e-mail containing personal data to the incorrect recipient)

5.5 unforeseen circumstances, such as damage to personal data due to a fire or flood

5.6 hacking, phishing and other "blagging" attacks where personal data is obtained by deceiving whoever holds it

5.7 alteration of personal data without permission; and

5.8 loss of availability of personal data.

6 If a Personal Data Breach is Discovered

6.1 If a member of staff knows or suspects that a personal data breach has occurred or may occur, they should inform their line manager and contact the DPO immediately.

6.2 Staff should not take any further action in relation to the breach. Staff must not notify any affected data subjects or regulators. The DPO will take appropriate steps to deal with the breach in collaboration with the Data Breach Team.

7 Managing and Recording the Breach

7.1 On being notified of a suspected personal data breach, the DPO will notify the Data Breach Team, consisting of the DPO, the Director, Head of Housing Services and the Corporate Services Officer. The Data Breach Team will be led by the DPO.

7.2 The Data Breach Team will take immediate steps to establish whether a personal data breach has in fact occurred. If so, the Data Breach Team will take appropriate action to:

7.2.1 contain the data breach and (so far as reasonably practicable) recover, rectify or delete the personal data that has been lost, damaged or disclosed.

7.2.2 assess and record the breach in the Index of Breaches.

7.2.3 notify appropriate parties (including the Information Commissioner's Office (ICO), Scottish Housing Regulator (SHR) and data subjects) of the breach; and

7.2.4 review the breach, its consequences and improvements that can be made.

These are explained in more detail below.

7.3 Containment and Recovery

7.3.1 The Data Breach Team will within 24 hours of knowledge, where possible, identify how the breach occurred and take immediate steps to stop or minimise further loss, destruction or unauthorised disclosure of personal data.

7.3.2 The Data Breach Team will identify ways to recover, correct or delete personal data. This may include contacting the Police if the breach involves stolen hardware or personal data.

7.3.3 Depending on the nature of the breach, the Data Breach Team will notify our insurer, as the insurer can provide access to data breach management experts, who may be able to assist us.

7.4 Assess and Record the Breach

7.4.1 Having dealt with containment and recovery within 48 hours of knowledge, the Data Breach Team will assess the risks associated with the breach, including:

(a) what type of personal data is involved?

(b) is the personal data, special category data?

(c) who is affected by the breach i.e. the categories and approximate number of data subjects involved?

(d) the likely consequences of the breach on affected data subjects (e.g. what harm could come to those data subjects, are there risks to their physical safety, reputation, or financial loss?)

(e) where personal data has been lost or stolen, are there any protections in place, such as encryption?

(f) what has happened to the personal data (e.g. if personal data has been stolen, could it be used for harmful purposes?)

(g) what could the personal data tell a third party about the data subject (e.g. could the loss of apparently trivial snippets of personal data help a determined fraudster build up a detailed picture of the data subject and result in e.g. identity theft?)

(h) what are the likely consequences of the personal data breach on our organisation (e.g. loss of reputation or liability for fines?)

(i) are there wider consequences to consider (e.g. loss of public confidence in an important service that we provide?)

7.4.2 Details of the breach will be recorded in the Index of Breaches by the Corporate Services Officer or another member of the Data Breach Team in their absence.

7.4.3 A member of the Data Breach Team should complete the Data Breach Blank Form and file as appropriate (see Appendix 1).

7.5 Notifying Appropriate Parties of the Breach

7.5.1 The Data Breach Team will consider whether to notify:

(a) the ICO

(b) affected data subjects

(c) the Police; and

(d) other parties, including the SHR.

7.5.2 Notifying the ICO

(a) The Data Breach Team will notify the ICO when a personal data breach has occurred, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of data subjects.

(b) Where ICO notification is required, this shall be done without undue delay and, where feasible, not later than 72 hours after we became aware of it. Where the notification to the ICO is not made within 72 hours, it will be accompanied by reasons for the delay.

(c) If the Data Breach Team is unsure whether to report, the presumption should be to report. The Data Breach Team will take account of the factors set out below:

The potential harm to the rights and freedoms of data subjects	This is the overriding consideration in deciding whether a personal data breach should be reported to the ICO. Detriments include emotional distress as well as both physical and financial damage. It can include: • exposure to identity theft through the release of non-public identifiers e.g. passport number; and • information about the private aspects of the data subject's life becoming known to

	others e.g. financial circumstances.
The volume of personal data	There should be a presumption to report to the ICO where: • a large volume of personal data is concerned; and • there is a real risk of data subjects suffering some harm. It will, however, be appropriate to report much lower volumes in some circumstances where the risk is particularly high (e.g. because of the circumstances of the loss or the extent of information about each data subject).
The sensitivity of personal data	There should be a presumption to report to the ICO where smaller amounts of personal data are involved, the release of which could cause a significant risk of data subjects suffering substantial detriment, including substantial distress. This is most likely to be the case where the breach involves special category data. In these circumstances, even a single record could trigger a report.

7.5.3 Notifying Data Subjects

(a) Where the personal data breach is likely to result in a high risk to the rights and freedoms of data subjects, the Data

Breach Team will notify the affected data subjects without undue delay, including:

(i) the name and contact details of the DPO from whom more information can be obtained

(ii) the likely consequences of the personal data breach; and

(iii) the measures we have or intend to take to address the personal data breach, including, where appropriate, recommendations for mitigating potential adverse effects.

(b) When determining whether and how to notify data subjects of the personal data breach, the Data Breach Team will:

(i) co-operate closely with the ICO and other relevant authorities (e.g. the Police); and

(ii) take account of the factors set out in the table below:

Factor	**Impact on obligation to notify data subject**
Whether we have implemented and applied (to the affected personal data) appropriate technical and organisational protection measures — in particular, measures that render the personal data unintelligible to any person who is not authorised to access it by e.g. encryption.	Where such measures have been implemented, it is not necessary to notify the data subject.
Whether we have taken measures following the personal data breach which ensure the high risk to	Where such measures have been implemented, it is not necessary to notify the

Factor	Impact on obligation to notify data subject
the rights and freedoms of data subjects affected by that breach is no longer likely to materialise.	data subject.
Whether it would involve disproportionate effort to notify the data subject.	If so, it is not necessary to notify the data subject — but we must instead issue a public communication or similar measure whereby the data subjects are informed in an equally effective manner.
Whether there are any legal or contractual requirements to notify the data subject?	If yes, it may be necessary to notify the data subject in any event.

7.5.4 Notifying the Police

The Data Breach Team will already have considered whether to contact the Police for the purpose of containment and recovery. Regardless of this, if it subsequently transpires that the breach arose from a criminal act, the Data Breach Team will notify the Police and / or relevant law enforcement authorities.

7.5.5 Notifying Other Parties

The Data Breach Team will consider whether there are any legal or contractual requirements to notify any other parties, such as the SHR. We must report certain notifiable events to the SHR, including a serious breach of legislation. Depending on the circumstances, and subject to the advice of the DPO, a personal data breach may be regarded as a serious breach of data protection legislation and may therefore constitute a notifiable event to the SHR. The prior advice of the DPO must be obtained by staff in such circumstances.

7.6 Reviewing the Breach and Improvements

Once the personal data breach has been handled in accordance with this Procedure, the Data Breach Team will within one month of handling the personal data breach:

7.6.1 establish what security measures were in place when the breach occurred

7.6.2 assess whether technical or organisational measures can be implemented to prevent the breach happening again

7.6.3 consider whether there is adequate staff awareness of security issues and look to fill any gaps through training or guidance

7.6.4 consider whether it is necessary to conduct a new, or revisit an existing, data protection impact assessment of the personal data processing that was the subject of the breach; and

7.6.5 update the risk register.

8 Staff Awareness and Training

8.1 Staff training and awareness raising is key to reducing the risks and occurrence of personal data breaches.

8.2 We provide regular data protection training to staff:

8.2.1 at induction

8.2.2 when there is any change to the law, regulation or our policy

8.2.3 when significant new threats are identified; and

8.2.4 in the event of a personal data breach occurring from which staff could learn.

9 Reporting Breaches

9.1 Prevention is always better than cure. Data security concerns may arise at any time, and we encourage staff to report any concerns to the DPO as soon as possible and at the earliest possible stage. This helps us capture risks as they emerge, protect us from personal data breaches, and keep our processes up-to-date and effective.

10 Consequences of Failure to Comply

10.1 Failure to comply with this Procedure puts us at risk. Failure to notify the DPO of an actual or suspected personal data breach is a very serious issue.

10.2 Staff may be liable to disciplinary action if they fail to comply with the provisions of this Procedure.

10.3 Due to the importance of this Procedure, failure to comply with any requirement of it will be actioned in line with the Disciplinary and Grievance Procedure. If an external organisation breaches this Procedure, they may have their contract terminated by us with immediate effect.

10.4 Any questions or concerns about this Procedure should be directed to the DPO.

11 Equalities

11.1 We are committed to ensuring equal opportunities and fair treatment for all people in our work. In implementing this Policy, we will provide a fair and equal service to all people, irrespective of factors such as gender, race, disability, age, sexual orientation, language or social origin, or other personal attributes.

12 Review

12.1 We will review and update this Procedure in accordance with our data protection obligations, and we may amend, update or supplement it from time to time and at least every 3 years or earlier, if required by changes in legislation.

Appendix 1 – Personal Data Breach Incident Report Form

Personal Data Breach Incident Record
Incident Number: DB

Please provide as much information as you can at this stage. Your initial response should be provided within 12 hours. Do not delay returning the form if you do not know the answers to all questions.

About the Breach

Please provide details of what happened, what went wrong and how it happened:

Was the breach caused by a cyber incident?

☐ Yes ☐No ☐Don't Know

How did you find out about the breach?

When did you discover the breach?
Date: Time:

When did the breach happen?
Date: Time:

Categories of personal data included in the breach (tick all that apply)

☐ Data revealing racial or ethnic origin
☐ Political opinions
☐ Religious or philosophical beliefs
☐ Trade union membership
☐ Sex life data
☐ Sexual orientation data
☐ Gender reassignment data
☐ Health data
☐ Basic personal identifiers, eg name, contact details
☐ Identification data, eg usernames, passwords
☐ Economic and financial data, eg credit card numbers, bank details
☐ Official documents, eg driving licences

☐ Location data
☐ Genetic or biometric data
☐ Criminal convictions, offences
☐ Not yet known
☐ Other (please give details below)

Number of personal data records concerned?

How many data subjects could be affected?

Categories of data subjects affected (tick all that apply)

☐ Tenant
☐ Occupant
☐ Applicant
☐ Employees
☐ Users
☐ Subscribers
☐ Students
☐ Customers or prospective customers
☐ Patients
☐ Children
☐ Vulnerable adults
☐ Not yet known
☐ Other (please give details below)

Potential consequences of the breach

Please describe the possible impact on data subjects because of the breach. Please also state the consequences of the breach on the organisation.

What is the likelihood that data subjects will experience significant consequences because of the breach?

☐ Very Likely
☐ Likely
☐ Neutral – neither likely or unlikely
☐ Unlikely
☐ Very Unlikely

☐ Not Yet Known

Please give details:

Had the staff member involved in this breach received data protection training in the last two years?

☐ Yes ☐No ☐Don't Know

If there has been a delay in reporting this breach, please explain why:

Describe any measures you had in place before the breach with the aim of preventing a breach of this nature (e.g. training has been given to all staff.)

Taking Action

Describe the actions you have taken, or propose to take, as a result of the breach. Include, where appropriate, actions you have taken to fix the problem, and to mitigate any adverse effects (e.g. confirmed data sent in error has been destroyed, updated passwords, planning information security training)

Outline any steps you are taking to prevent a recurrence, and when you expect they will be completed (e.g. refresher training has been carried out)

Have you told data subjects about the breach?

☐ Yes, we've told all affected data subjects.
☐ We're in the process of telling all affected data subjects.
☐ No, they're already aware.
☐ No, but we're planning to.
☐ No, we've decided not to.

☐ We haven't decided yet.
☐ Something else (give details below).

Have you told, or are you planning to tell any other organisations about the breach? (e.g. the ICO, the police, other regulators or supervisory authorities)

☐ Yes ☐No ☐Don't Know

If you answered yes, please specify:

Authorisation

Actions agreed by

_____ _____
Director Date

Notes

Equalities Impact Assessment

Policy/Project/Service Information			
Lead Officer	Corporate Services Officer		
Policy / Project / Service	Data Breach Management Procedure	**New Policy / Project / Service or revision of existing?**	New policy
Is this a reassessment following amendments being required at a previous assessment?	No		
Briefly describe the aims, objectives and purpose of the policy / project / service.	Places obligations on staff to report actual or suspected personal data breaches and sets out our procedure for managing and recording actual or suspected personal data breaches.		
Who is intended to benefit from the policy / project / service? (E.g. applicants, tenants, staff, contractors)	All stakeholders and data subjects		
What outcomes are wanted from this policy / project / service? (E.g. the measurable changes or benefits to members/ tenants / staff)	To ensure personal data is kept secure against loss or misuse. To further ensure that WWHC is compliant with legislation and Regulatory Standards.		

Consultation
Who have you engaged and consulted with as part of your assessment? N/A

Equalities Impact Assessment		
Which protected characteristics could be	**Identify any positive impact/s**	**Identify any negative**

affected by the policy, practice, or service?		that could result for each of the protected characteristic groups.	impact/s that could result for each of the protected characteristic groups.
Age	**x**	Seeks to ensure any data breach (suspected or actual) is handled correctly and that breaches are contained to not cause further harm/distress and that notification procedures are in place.	Failure to handle breaches properly could result in further harm/distress for data subjects and result in loss of trust or damaged reputation.
Disability	**x**	"	"
Gender Reassignment	**x**	"	"
Marriage & Civil Partnership	**x**	"	"
Race	**x**	"	"
Religion/Belief	**x**	"	"
Pregnancy/Maternity	**x**	"	"
Sex	**x**	"	"
Sexual Orientation	**x**	"	"

Action Plan To Mitigate Negative Impact		
What action/s are required to address the impacts arising from this assessment?		
Protected characteristics	**Action**	**Implementation Date**
Age	Staff training and publication of this policy to ensure all staff are aware of their responsibilities under GDPR. Ensure policies and procedures are reviewed regularly to ensure up-to-date practices and follow recommendations from software/IT providers.	Ongoing
Disability	"	

Gender Reassignment	“	
Marriage & Civil Partnership	“	
Race	“	
Religion/Belief	“	
Pregnancy/Maternity	“	
Sex	“	
Sexual Orientation	“	
Human Rights	“	

Final Decision	**Tick relevant box**	**Include explanation where appropriate**
Approved for implementation without change		
Amend or change the Policy/Project/Service		
Continue the Policy/Project/Service without change (despite impact)		
Stop the Policy/Project/Service		

Lead Officer Signature	R.Hosie
Date	17/03/2026
Date approved by Management Committee/ Sub Committee	20/03/2026