Copies of all Elizabeth Finn Homes Limited (EFHL) HR Policies can be found on the EFHL Intranet. All EFHL employees are subject to EFHL HR Policies. EFHL HR Policies are non-contractual, are reviewed regularly and may be subject to change. All queries on the application or interpretation of this policy should be raised with the Head of Department or HR.

10.5 – Data Breach

Purpose

This policy is designed to ensure EFHL, its employees, agents and contractors can identify data breaches and meet the requirements of Data Protection Legislation in the handling of a personal data breach (henceforth "data breach").

Data Protection Legislation means the amended Data Protection Act 2018 (UK GDPR), the Privacy and Electronic Communications (EC Directive) Regulations 2003 and any legislation implemented in connection with the Data Protection Act 2018 (UK GDPR). This includes any replacement legislation coming into effect from time to time. Where appropriate for EU residents, good or services, it includes EU GDPR.

Definitions

a. Any reference to "Article" or "Articles" is a reference to an Article or Articles of the Data Protection Act 2018 (UK GDPR).

b. The terms 'personal data', 'data subject', 'processing', 'pseudonymisation', 'controller', 'processor', 'recipient', 'third party', 'consent', 'personal data breach', have the meanings set out in Article 4 of the Data Protection Act 2018 (UK GDPR).

c. "Security incident" means an incident in which the security of personal data *may* have been compromised but no risk is identified in respect of the rights and freedoms of data subjects. Security incident in the context of this policy may also be used to define an event or action which *may* compromise the confidentiality, integrity or availability of systems or data, where such event or action does not presently amount to a reportable data breach.

What is a data breach?

A data breach is defined within the Data Protection Legislation as "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".

The notification requirements associated with data breaches rest on the level of risk to the rights and freedoms of data subjects arising from the breach. Unless a data breach is unlikely to result in a risk to the concerned data subjects, it is to be reported to the ICO or relevant supervisory authority. Where such data breaches are likely to result in a high risk to the rights and freedoms of the concerned data subjects, the affected data subjects are to be informed in addition to the supervisory authority. The ICO provide details on this, including a matrix to help asses what is reportable.

The Data Protection Legislation further stipulates that where notification of the supervisory authority is required, this should take place within 72 hours of the controller becoming aware of the data breach. In the case of breaches which pose a high risk to data subjects, the

Issued Jan 2020
Reviewed: Jan 2020, Jun 2021, May 2023
Revised:Jul 2021 (minor changes for UK GDPR), May 2023 (minor)

additional requirement to notify data subjects must be done as soon as possible without undue delay.

In light of these requirements, this policy focuses on the responsibilities of all employees, agents and contractors associated with EFHL in internally reporting breaches and the company external notification requirements.

Responsible Persons
The Directors of the organisation have responsibility for ensuring that any privacy risks are managed.

All users of information assets across the organisation should familiarise themselves with this procedure, be aware of privacy risks and be vigilant in order to ensure breaches are identified, reported and managed in a timely manner.

All staff are responsible for reporting mistakes, suspected or actual data breaches at any given time. They must report all incidents, including those resulting from human error and those with unidentified or unknown affected data subjects as soon as detected.

Support will be provided to ensure everyone has access to the appropriate skills and training to carry out their role effectively. However gross negligence and intentional violations (including not reporting incidents/mistakes) are taken seriously and could lead to disciplinary action.

Breach Response Processes

a) Identify the breach

Personal data breaches could include:

- access by an unauthorised third party;
- deliberate or accidental actions by EFHL, its processors or their employees, agents or contractors;
- human error affecting personal data
- sending personal data to an unauthorised recipient;
- network intrusions
- loss or theft of confidential or sensitive data or equipment on which such data is stored (e.g. loss of laptop, USB stick, iPad / tablet device, or paper record);
- alteration of personal data without permission;
- loss of availability of personal data

b) Report the Breach

10.5 – Data Breach

When reporting a security incident or personal data breach, suspected or actual, the reporter (employee, relative, contractor etc) is obliged to disclose all information within their knowledge using the **Breach Report Form** annexed to this Policy (Annex 1).

This must be submitted to the Home Manager and the Data Protection Lead immediately.

The Home Manager and the Data Protection Lead will analyse the form, update the Data Breach Register, investigate the breach and ascertain whether any immediate corrective, containment or escalation actions are required.

c) Investigate the Breach

EFHL aims to complete a preliminary investigation of all reported incidents without undue delay, with an aim to establish its awareness of a personal data breach within the **first 24 hours** of internal detection.

From that point, EFHL has **72 hours** within which to identify whether there is a risk to the concerned data subjects and where there is a risk, notification to the supervisory authority should take place.

During the investigation, EFHL aims to establish the following:

- The facts of the security incident
- The data or records concerned
- The value and sensitivity of the data or records concerned
- The type of breach suspected (confidentiality, availability, integrity)
- The number and identity of affected data subjects
- To identify and assess the ongoing risks that may be associated with the breach. In particular, an assessment of;
  (a) potential adverse consequences for individuals,
  (b) their likelihood, extent and seriousness.
- The measures required to contain the impact of the breach

Determining the level of risk will help define actions in attempting to mitigate those risks and EFHL's notification responsibilities.

d) Notify the Supervisory Authority

EFHL aims to ensure that all data breaches which pose a risk to the rights and freedoms of data subjects will be reported to the Information Commission's Office (ICO) within 72 hours of becoming aware of a relevant breach.

All notifications to the ICO must be made with the authorisation of an executive employee of EFHL and will be made using the breach notification form provided by the ICO.

e) Notify the affected Data Subjects

Where a high risk to the rights and freedoms of data subjects is established in the Risk Assessment, EFHL will inform data subjects of the personal data breach as soon as possible and without undue delay.

Communication to data subjects should include:

- The nature of the breach;
- The name and contact details of the Data Protection Lead or other contact person;
- The likely consequence of the breach;
- The measures taken or proposed to be taken by the controller to address the breach
- any recommended steps to be taken by the data subjects themselves e.g. changing passwords.

EFHL aims to notify data subjects of relevant personal data breaches directly unless it is impossible to do so, or it would involve a disproportionate effort, in which case the breach may be communicated by way of a public statement. All such communications must be authorised by an executive employee.

f) Notify Others

Consider, as necessary, the need to notify any third parties who can assist in helping or mitigating the impact on individuals.

These could be police, other regulatory or supervisory authorities, insurers, professional bodies, funders, trade unions, website/system owners, bank/credit card companies.

This list is not exhaustive.

Accountability
All security incidents reported will be documented regardless of whether the breach was notifiable to the ICO. EFHL will maintain a Data Breach register containing all reported incidents.

Evaluation
The Data Protection Lead will evaluate the effectiveness of EFHL's response to the breach to learn and apply any lessons or remedies or recommendations in the light of findings or experience across the organisation.

Copies of all Elizabeth Finn Homes Limited (EFHL) HR Policies can be found on the EFHL Intranet. All EFHL employees are subject to EFHL HR Policies. EFHL HR Policies are non-contractual, are reviewed regularly and may be subject to change. All queries on the application or interpretation of this policy should be raised with the Head of Department or HR.

10.5 – Data Breach

Annex 1

Please complete this form if you have detected or been advised of a data breach. It is imperative that you complete this form immediately upon detection and where possible, please advise your line manager of the suspected breach immediately.

Once completed, please email this form to hradmin@efhl.co.uk and it@efhl.co.uk with the subject DATA BREACH in the subject field.

Incident / breach details	
Name of person reporting incident:	
Contact details of person reporting incident:	
Date(s) incident took place:	
Date you detected the incident:	
Place of incident:	
Brief description of how you became aware of the incident:	
Brief description of the incident including details of the data, records or systems believed to be affected:	
Approximate number of affected data subjects, if known:	
Approximate number of affected records, if known:	
Any actions taken in response to the incident:	

Issued Jan 2020
Reviewed: Jan 2020, Jun 2021, May 2023
Revised:Jul 2021 (minor changes for UK GDPR), May 2023 (minor)