

DATA SECURITY POLICY

This policy outlines behaviours expected of employees when dealing with data and provides a classification of the types of data with which they should be concerned.

The induction process for new employees will be provided with Data Security Training, Acceptable Use Policy Monitoring & Surveillance Policy to provide users with guidance on the required behaviours.

Purpose

Higham must protect restricted, confidential or sensitive data from loss to comply with GDPR regulations, avoid reputation damage and to avoid adversely impacting our customers. The protection of data in scope is a critical business requirement, yet flexibility to access data and work effectively is also critical.

It is not anticipated that this technology control can effectively deal with the malicious theft scenario, or that it will reliably detect all data. Its primary objective is user awareness and to avoid accidental loss scenarios. This policy outlines the requirements for data leakage prevention, a focus for the policy and a rationale.

Scope

Any employee, contractor or individual with access to Higham systems or data.

Definition of data to be protected

- Financial
- Restricted/ Sensitive (eg: quotations)
- Confidential / Personal

Policy - Employee requirements

1. Higham employees complete Data Security Awareness Training and agree to uphold the Acceptable Use Policy, Monitoring & Surveillance Policy which will be signed for at the process of induction with Higham. Interim / acceptable and ongoing training will also continue. These may be in the form of Tool Box Talks, specified training by governing bodies, change of law and is regarded as part of employee continual improvement process.
2. If employees identify an unknown person, un-escorted or otherwise unauthorised individual on a Higham site they shall immediately notify the site supervisor and if appropriate Joseph Monaghan.
3. Visitors to Higham sites will be escorted by an authorised employee at all times. Employees responsible for escorting visitors will restrict them appropriate areas.
4. Higham employees are required not to reference the subject or content of sensitive or confidential data publically, or via systems or communication channels not controlled by Higham. For example, the use of external e-mail systems not hosted by Higham to distribute data is not allowed.
5. Employees are to keep a clean desk / site office. To maintain information security employees will ensure that all printed data of a sensitive nature is not left unattended. Employees are to ensure drawers, lockers, cabinets and site cabins are left locked and only authorised personnel allowed access.

6. You need to use a secure password on all Higham systems as per the Higham password guidance. These credentials must be unique and must not be used on other external systems or services.
7. Terminated employees will be required to return all records, in any format, containing financial, restricted / sensitive or confidential/personal information.
8. Higham employees must immediately notify Joseph Monaghan in the event that a device containing in scope data is lost (e.g. mobiles, laptops, smart phones etc).
9. In the event that employees find a system or process which they suspect is not compliant with this policy or the objective of information security they have a duty to inform Joseph Monaghan so that appropriate action can be taken.
10. If Higham employees have been assigned the ability to work remotely they are to take extra precautions to ensure that data is appropriately handled. Seek guidance from Joseph Monaghan if you are unsure as to your responsibilities.
11. Higham employees are to ensure that assets holding data in scope are not left unduly exposed, for example visible on the seat of a car / van.
12. Data that must be moved within Higham is to be transferred only via business provided secure transfer mechanisms (e.g. encrypted USB keys, file shares, email etc). Higham will provide employees with systems or devices that fit this purpose as required. Employees must not use other mechanisms to transfer data. If employees have a query regarding use of a transfer mechanism, or it does not meet the business purpose they are to raise this with Joseph Monaghan, Managing Director.

Enforcement

Any Higham employee found to have violated any of the policies and procedures outlined may be subject to disciplinary action in line with the terms of the Employee Handbook.

Signed: 
Director
On behalf of Higham Flat Roofing Ltd