

This Data Breach Summary explains how West Heanton identifies, contains, assesses and reports personal data breaches, and the steps we take to protect personal information.

Purpose of This Summary

West Heanton Ltd is committed to protecting personal information and responding quickly and appropriately if a personal data breach occurs.

This summary supports our wider GDPR approach and should be read alongside our data protection, privacy, security and team policies.

What Is a Personal Data Breach?

A personal data breach is a security incident that leads to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

- Examples include sending personal data to the wrong recipient.
- Loss or theft of paper records, devices or equipment containing personal data.
- Unauthorised access to systems, files, email accounts or records.
- Accidental deletion, corruption or loss of access to personal data.
- Cyber incidents such as malware, phishing, compromised passwords or ransomware affecting personal data.

A breach may be accidental or deliberate. It may affect the confidentiality, integrity or availability of personal data.

Identifying and Escalating a Breach

All team members are expected to recognise potential data breaches and report them immediately to the Data Protection Officer or the appropriate manager.

- Team members should report suspected breaches as soon as they become aware of them.
- The report should include what happened, when it happened, the data involved and who may be affected.
- Team members should preserve relevant evidence and avoid deleting emails, logs, files or records connected with the incident.
- Where a supplier or processor identifies a breach, they should notify West Heanton without undue delay.
- The Data Protection Officer or appointed manager will coordinate the response and maintain a breach record.

Containing the Breach

Once a breach is identified, West Heanton will take prompt action to limit the impact and protect individuals.

- Recover, recall or secure the affected information where possible.
- Ask unintended recipients to delete, return or securely dispose of information sent in error.
- Disable compromised accounts, reset passwords and restrict access where required.

- Isolate affected devices, systems or files to reduce further risk.
- Preserve evidence so the cause and impact can be investigated.

The priority is to reduce harm, protect affected individuals and prevent further unauthorised access, loss or disclosure.

Assessing Risk

West Heanton will assess each breach to understand what happened, what personal data was affected, how many individuals may be involved and the likely consequences for those individuals.

The assessment will consider the sensitivity of the data, whether it is protected, who has access to it, the likelihood of misuse and whether the breach may result in harm such as distress, identity theft, financial loss, discrimination, reputational damage or loss of confidentiality.

Reporting and Notification

Where a personal data breach is likely to result in a risk to the rights and freedoms of individuals, West Heanton will report it to the Information Commissioner's Office without undue delay and, where feasible, within 72 hours of becoming aware of it.

Where a breach is likely to result in a high risk to affected individuals, West Heanton will inform those individuals without undue delay and provide appropriate information to help them protect themselves.

Recording Breaches

West Heanton will keep an internal record of personal data breaches, including breaches that do not need to be reported to the Information Commissioner's Office.

The record should include the facts of the breach, the personal data involved, the individuals affected, the assessment of risk, actions taken, notification decisions and any follow-up measures.

Preventing Future Breaches

After a breach, West Heanton will review the incident and identify practical steps to reduce the risk of similar breaches happening again.

- Actions may include team training, updated procedures, stronger access controls, password resets, improved system monitoring, better supplier oversight, encryption, secure disposal and revised retention practices.
- Lessons learned will be shared with relevant team members where appropriate.
- Any recurring issues will be reviewed by management and addressed through corrective action.

Review of This Summary

This Data Breach Summary will be reviewed periodically and updated where necessary to reflect changes in law, guidance, working practices or organisational responsibilities.

Contact Us

If you have any questions about this Data Breach Summary or wish to report a suspected personal data breach, please contact our Data Protection Officer at office@westheanton.co.uk.