Q2.16 Information Security Policy

Emily Price

Introduction

This policy outlines the measures to protect Kingsley Plastics Ltd's IT systems from damage and threats, whether internal, external, deliberate, or accidental.

Key Principles

1. **Protection Against Unauthorised Access**
    - IT systems must be protected against unauthorised access.
    - Use IT systems in compliance with relevant company policies (e.g., Data Protection Policy).
2. **Data Management**
    - Securely manage all data in compliance with data protection laws.
    - Classify and handle data appropriately (e.g., personal data, sensitive data).
    - Ensure data is accessible only to those with a legitimate need. A legitimate need is established either by a pre-authorised clearance from a known requirement of their job role, or by a legal right.
3. **IT System Maintenance**
    - IT systems must be installed, maintained, and upgraded by authorised personnel.
    - The IT Department is responsible for the security and integrity of IT systems and data.
4. **Reporting Security Concerns**
    - Report any security concerns immediately to the Managing Director or the Technical Director.
    - If concerns involve personal data, also report to the Data Protection Officer.

IT Department Responsibilities

- Ensure IT systems meet security requirements.
- Implement and review IT security standards.
- Provide support and training to users on IT security.
- Manage access levels based on job roles.
- Ensure regular data backups are taken and stored securely.
- The Managing Director holds a secure record of passwords for emergency access to devices and systems. Passwords should never be shared with any other person.

User Responsibilities

- Comply with this policy and related policies.
- Use IT systems within the bounds of UK law.
- Report security concerns and technical problems immediately.
- Do not install unauthorised software.

Software Security Measures

- Keep all software up-to-date with relevant updates and patches.
- Fix or withdraw software with security flaws.
- Only install approved software.

Anti-Malware Security Measures

- Protect IT systems with suitable anti-malware software.
- Scan all physical media and files for malware.
- Report any detected malware immediately.

Hardware Security Measures

- Secure IT systems in locked rooms or cabinets.
- Physically secure non-mobile devices.
- Transport and handle mobile devices securely.

Access Security

- Determine access privileges based on job roles.
- Protect IT systems with secure passwords.
- Only share passwords with the Managing Director.
- Report any suspected breaches.

Data Storage Security

- Store data securely using passwords and locked storage.
- Do not store personal data on mobile devices without approval.

- Ensure data transferred to personal devices complies with data protection policies.

Data Protection

- Handle personal data in compliance with data protection laws and company policies.
- Encrypt and mark emails containing personal data as confidential.
- Transmit personal data over secure networks only.

Internet and Email Use

While at work, while using a company device, or Kingsley associated profile:

- Only use the internet and communications platforms (such as email and social media), for the express benefit of the company, to uphold our reputation.
- Act in a legal, professional and ethical manor befitting an employee and representative of the company.
- Take additional steps to ensure IT security when using the internet or email.

Reporting IT Security Breaches

- Report all security concerns and breaches to the IT Department and to Mark Manley, Managing Director.
- Do not attempt to resolve breaches without consulting the IT Department.

This policy is approved by the undersigned and is supported by all the levels of management within the organisation. All personnel shall be guided by the contents of the SHEQ Management System and no deviation from the methods and procedures set down shall be permitted. This policy is under continuous review.

Name - Mark Manley

Role - Managing Director

Date - 14/05/2025