



Cyber security and keeping your data safe

At Finsbury Food Group, protecting data and maintaining operational resilience are core priorities. We take a structured, risk-based approach to cyber security, combining preventative controls, monitoring capability and continuous staff awareness.

Overview

In a world where technology is rapidly advancing, cybersecurity is more important than ever. Keeping our data safe, systems protected, and networks secure is a top priority. At Finsbury Food Group, everyone plays an important part in keeping our team cybersecure. If you have any questions or concerns surrounding cybersecurity, contact a member of the FFG team who are always happy to answer questions.

What is the problem that needs resolving in industry?

We treat cyber vigilance with the same seriousness as Food Safety and Health & Safety. In an ever-evolving cyber security landscape it's important we react accordingly to new threats and be proactive in preparing the business using the principles of:

Prevention

Goal: To stop threats from entering or impacting systems in the first place.

Examples: Firewalls, antivirus, strong authentication and security awareness training.

Detection

Goal: To identify malicious activity, whether known or unknown, that bypasses prevention.

Examples: Network monitoring, Endpoint Detection and monitoring endpoint behaviours.

Response

Goal: To contain, neutralise, and eradicate threats once detected, minimizing damage.

Examples: Incident response plans and Business Crisis Plans that are tested regularly to ensure they are current and effective.

These are governed by National Crime Security Centre frameworks like Cyber Assessment Framework and Cyber Essentials which are government backed certification schemes.



Finsbury Food Group Targets or Business Plan



The main points we need to focus on to ensure a safe network and securing yours and our data:

- Using secure software, including sharing tools, monitoring systems and password managers.
- Only Connecting trusted devices to ensure our network stays secure, which means IT-approved devices.
- Monitoring and logging activity, so that we can maintain your safety, and ours online.

What can customers do?

- Update operating systems – keep your systems modernised .
- Remote access – use multi-factor authorisation.
- Strengthen email security and network protection.
- Use strong password protection management.
- Ensure safety when sharing content with suppliers & customers with secure software.
- Only use trusted IT-approved devices.
- Have strong password management systems.

At Finsbury Food Group, cyber security awareness is embedded across the organisation through a structured and ongoing programme. This includes:

- Mandatory cyber security training for all employees, with annual refreshers.
- Regular internal communications and updates on emerging cyber threats.
- Simulated phishing exercises to reinforce learning and improve awareness.
- Targeted guidance for higher-risk roles and privileged users.

**Bakery
brilliance
makes every
day special.**

