Glossary

General & Cyber Terms

Data Breach - When private or confidential information is accidentally or deliberately shared with unauthorised people.

Sensitive information – Personal details, medical records, or any confidential data that must be kept secure.

Email & Security Terms

Multi-Factor Authentication (MFA) – A security feature that asks for more than just a password (like a text message code) before allowing access e.g., your bank asking to send you a text message to log in.

Email encryption – A security method that makes emails unreadable to anyone except the intended recipient.

Phishing – A fake email, message, or website designed to trick people into sharing passwords or clicking harmful links.

Recall an email – An attempt to pull back a sent email before the recipient reads it (often unreliable).

Cyber Attack & IT System Terms

Ransomware – A type of cyber attack that locks files or systems until a ransom is paid.

Backup – A copy of important files stored safely in case the originals are lost or locked by hackers.

Business Continuity Plan – A plan for how to continue working if IT systems fail or are attacked.

Incident Response Plan/Policy – An organisation's official plan for handling cyber security problems or data breaches.

Legal & Compliance Terms

ICO (Information Commissioner's office) – The UK authority responsible for data protection and investigating breaches.

Compliance – Following laws, rules, or policies to keep data and systems secure.

Regulatory Issues – Problems that could get the organisation in trouble with the law or official regulators.

Technical Workarounds & Risks

Unofficial Workarounds – Using personal devices, writing things down, or finding alternative ways to work when systems fail (can be risky).

Troubleshooting – Basic steps like restarting a computer or checking connections to fix simple IT problems.

Secure Portal – A safe online system for sharing sensitive documents instead of using email.