Ectron Limited: IT Use Policy

1.0 Introduction and purpose

This policy governs the use of all information technology (IT) resources owned or operated by Ectron Limited. This includes, but is not limited to, computers, laptops, servers, networks, software, internet access, email, mobile devices, and telecommunications equipment.

The purpose of this policy is to:

Ensure the security, integrity, and confidentiality of Ectron's data and systems.

Provide a clear framework for the appropriate and acceptable use of all IT resources.

Ensure compliance with UK laws and regulations, including the UK General Data Protection Regulation (UK GDPR).

Protect Ectron Limited and its employees from legal liability and reputational damage.

2.0 Scope

This policy applies to all employees, directors, contractors, temporary staff, and any third parties who are granted access to Ectron Limited's IT resources.

3.0 General principles

Property of Ectron Limited: All IT resources and the data stored on them are the property of Ectron Limited. Users should not expect a right to privacy when using company IT equipment, and Ectron reserves the right to monitor usage in accordance with UK law and this policy.

Monitoring and consent: By using Ectron's IT resources, employees consent to their use being monitored for policy compliance and security purposes. Monitoring may be necessary to counter misuse and ensure the security of the network.

Business use first: All IT resources are provided primarily for legitimate business purposes. Limited and reasonable personal use is permitted during break times, provided it does not interfere with job duties, consume excessive network resources, or breach any other part of this policy.

Security awareness: All users are responsible for protecting the company's IT resources and sensitive data. All staff will receive regular security awareness training.

4.0 Acceptable and unacceptable use

4.1 Acceptable use

Using email and internet access for legitimate business communications and research.

Accessing and processing data required for your job function, in accordance with the Data Protection Policy.
Using company-provided software and applications for approved work tasks.

4.2 Unacceptable use

Illegal or criminal activity: Accessing, storing, or transmitting illegal, obscene, or offensive materials. This includes any content that is discriminatory, defamatory, harassing, or in violation of copyright law.
Security breaches: Attempting to circumvent security measures, including installing unauthorised software, disabling antivirus, or attempting to gain unauthorised access to systems.
Misuse of resources: Engaging in activities that waste IT resources, such as excessive personal internet browsing or the downloading of non-work-related large media files.
Breach of confidentiality: Disclosing confidential or proprietary company information, including personal data, without authorisation.
Misrepresentation: Creating or sending material that misrepresents your identity or attempts to impersonate another user.
External media: Using external storage media (e.g., USB drives, external hard drives) on company equipment without prior authorisation from IT.

5.0 Email and internet

Email communication: Employees must use appropriate and professional language in all email communications. Offensive, threatening, or harassing content is strictly prohibited.
Personal email: Personal email accounts must not be used for conducting company business.
Phishing and scams: Users must be vigilant and report any suspicious emails immediately to the IT department.
Internet browsing: Access to certain websites may be blocked by company filters. Users should not attempt to bypass these filters.

6.0 Data protection

UK GDPR compliance: All personal data processed using company IT resources must be handled in strict accordance with Ectron's Data Protection Policy and the UK GDPR.
Access controls: Access to sensitive or personal data is restricted to employees who require it for their job function.
Reporting breaches: Any suspected or actual data breaches must be reported immediately to management and the Data Protection Officer (DPO).
Retention and disposal: All company data should be stored and disposed of in line with the company's data retention schedule.

7.0 Security responsibilities

User IDs and passwords: Users are responsible for keeping their user IDs and passwords confidential. Passwords must be strong, changed regularly, and never written down or shared.
Device security: Employees must lock their computer screens when leaving their workstations. All company devices, including laptops and mobile phones, must be kept secure at all times.
Reporting incidents: Any suspected security incidents, such as a lost device or a compromised password, must be reported to the IT department immediately.

8.0 Mobile devices

Company-owned devices: Company-provided mobile devices are for business use. Any personal use is subject to the same rules as other IT equipment.
Personal devices (BYOD): The use of personal devices for company business is not permitted unless explicitly authorised. If allowed, users must follow specific security protocols.

9.0 Social media

Professional conduct: When using social media, especially in a way that identifies you with Ectron Limited, employees must act professionally and not post anything that could damage the company's reputation.
Confidentiality: Do not discuss company business, customers, or confidential information on social media.
Authorised accounts: Only designated individuals are authorised to post on Ectron Limited's official social media accounts.

10.0 Consequences of breach

Any breach of this policy may result in disciplinary action, which could include the withdrawal of access to IT resources, or, in cases of gross misconduct, dismissal. Breaches that are illegal may also result in criminal prosecution.

11.0 Policy review

This policy will be reviewed annually and updated as necessary to reflect changes in technology, business practices, and legal requirements.

On behalf of Ectron Limited

Mr. A Jones, Director.