IT USAGE POLICY

1. **Introduction -** This policy defines the acceptable use of IT equipment, systems, cloud services, mobile devices, and artificial intelligence (AI) tools at Jones Bros Ruthin (Civil Engineering) Co. Ltd. It is designed to protect users and the company from modern cyber threats including phishing, malware, social engineering, insider misuse, and emerging technologies. The policy supports compliance with ISO/IEC 27001 and the UK Government's Cyber Essentials framework.

   Internet Usage - Internet access is provided for work-related activities. Brief personal use is allowed if it is not excessive, inappropriate, or in breach of any part of this policy. **Do not:**

   - Access or share indecent, obscene, racist, or defamatory material
   - Register on websites using your company email except for authorised business
   - Download or share copyrighted content (e.g. music, films, software)
   - Use company networks for streaming, gaming, or personal shopping
   - Install unapproved software
   - Bypass security settings or attempt to access restricted content

   Use of mobile data or Wi-Fi devices must be business-related. Minimal personal use is acceptable if compliant.

   If you are using a mobile Wi-Fi device to access the internet, please make sure that any downloaded data is work related. Brief and occasional personal use of the Jones Bros Wi-Fi devices to connect to the Internet is acceptable as long as it is not excessive or inappropriate and does not conflict with any other aspect of this policy.

2. **Email Use-** Company email is strictly for work purposes. **You must:**

   - Only use your Jones Bros email for business communications
   - Never use personal email accounts for work purposes or install them on company devices
   - Never register personal accounts or services with your company email
   - Avoid forwarding chain letters, hoaxes, or inappropriate content
   - Compress large attachments where possible
   - Report any suspected phishing attempts immediately
   - Do not click suspicious links or open unexpected attachments. Report potential phishing to IT immediately.

   Phishing and Cyber security training is mandatory.

3. **AI Use -** Use of artificial intelligence tools must be pre-approved by the IT Department. **Do not:**

   - Input confidential, personal, or sensitive information into public AI tools
   - Use AI to make decisions in safety-critical, financial, or contractual situations
   - Assume AI-generated content is accurate, copyright-free, or safe to use
   - Use AI tools to record, transcribe, or analyse a meeting unless all attendees have explicitly agreed to their use and understand how the data will be stored and protected

   Permitted - Use of approved AI tools for work-related efficiency (e.g. summarising documents) where outputs are reviewed before use

   Unapproved use of AI may result in disciplinary action.

4. **Cloud Services -** Use of cloud storage and services must follow company standards. **You must:**

    - Use only authorised cloud platforms (e.g. company-managed OneDrive, SharePoint)
    - Not store work files in personal cloud accounts (e.g. personal Dropbox, Google Drive)
    - Use MFA to access all cloud services
    - Follow company data classification and encryption guidance for sensitive files

    Cloud use must align with our Data Protection and Security Policies.

5. **File Sharing and Software -** Jones Bros recognises that secure file sharing is essential for collaboration across offices, project sites, and with approved third parties. **You must:**

    - Use only company-approved platforms such as Microsoft SharePoint, OneDrive, or other authorised systems for sharing files internally and externally.
    - Follow company guidance for setting appropriate permissions, including read-only or time-limited access where required.
    - Use password protection or encryption for sensitive or confidential files when sharing with external parties.
    - Contact the IT Department if you require support setting up secure links, permissions, or shared folders.

You must not:

- Use personal file sharing services such as Dropbox, Google Drive, WeTransfer, or similar without written approval from IT
- Share links that bypass company security or allow uncontrolled public access
- Circumvent existing file sharing processes by using unapproved apps, USB drives, or email to transfer large or sensitive data sets
- Install any software without IT approval
- Use file sharing software such as BitTorrent, uTorrent, or any other peer-to-peer sharing applications
- Use unlicensed or unauthorised software

Report immediately if you believe your device has allowed unauthorised software installation. Secure file sharing reduces the risk of data breaches and ensures compliance with data protection legislation.

6. **Mobile Device Use -** Company smartphones and tablets are for business use. Minimal personal use is permitted. **Rules:**

    - Use protective cases at all times
    - Set strong PINs (not 1234, 1111, etc.)
    - Do not use company SIMs abroad without manager approval
    - Contact IT for high-data tasks if required
    - All data usage on work devices may be monitored
    - Only authorised apps may be installed and used on company mobile devices. Installation of unapproved apps is not permitted

7. **Passwords and Access - You must:**

    - Use strong passwords (minimum 12 characters, avoid dictionary words)
    - Enable MFA where available (mandatory for cloud services)
    - Never share your password or write it down visibly
    - Log out or lock your PC when leaving your desk

    Use of unauthorised equipment (e.g. personal laptops) on the company network is forbidden.

8. **Data Handling and Protection -** All data must be stored securely. **You must:**

   - Save work on the Pansophy system and or pre – approved and authorised team SharePoint sites only, not local drives
   - Use secure channels for data transfer (e.g. encryption, secure links)
   - Not email sensitive data unencrypted
   - Treat all company data as confidential unless labelled otherwise
   - Use encryption for removable media or avoid use where not authorised
   - Adhere to all data protection principles under UK GDPR.

9. **Security Threats and Incident Response -** Examples of threats include:

   - Phishing emails
   - Ransomware or malware infections
   - Social engineering (e.g. suspicious phone calls)
   - Insider misuse
   - Cloud misconfiguration or AI misuse

   If you suspect a threat:

   - Report it to IT immediately via email or phone
   - Disconnect your device if a ransomware or malware infection is suspected
   - Report lost or stolen devices immediately

   No blame culture: reporting immediately or when you become aware is encouraged to limit impact.

10. Circumventing Security Protocols - You must not attempt to bypass, disable, or otherwise circumvent any security controls that have been put in place to protect company systems. This includes but is not limited to:

    - Attempting to access blocked or restricted websites
    - Using virtual private networks (VPNs), proxy servers, or similar tools to hide activity or access unauthorised content
    - Attempting to interfere with antivirus, endpoint detection, or firewall settings

    Any attempt to circumvent security protocols will be considered a serious breach and may result in disciplinary action.

11. **Tampering with IT Equipment and Server Cabinets -** All IT server equipment, whether in head office, regional offices, or project sites, must not be tampered with under any circumstances.

    - Do not attempt to open, remove, disconnect, or modify any server or network cabinet equipment
    - Project site IT installations are fitted with internal monitoring cameras to prevent tampering. These cameras only record when the cabinet is opened and are positioned so that they only capture the interior of the cabinet and the face of the individual opening it. No audio is recorded.

    Any unauthorised access or tampering will be logged and investigated. Disciplinary action will follow where necessary.

12. **Unauthorised Devices -** Only authorised IT equipment may be connected to the company network.

    - Personal laptops, USB drives, external hard drives, smartphones, or any other devices must not be plugged into company computers, servers, or network points without prior written approval from the IT Department
    - This includes charging personal devices via company equipment using USB connections

Connecting unauthorised devices poses a security risk and may lead to malware infection or data compromise. Breaches of this rule will be investigated.

13. **Monitoring and Compliance -** Your activity on company systems is monitored for security, compliance, and performance. Breaches of this policy may result in disciplinary action. IT may access company IT devices to support investigations or service delivery.

14. **Training and Awareness -** All employees with access to company IT assets must complete mandatory security awareness training annually. This includes:

    - Phishing and social engineering
    - Password hygiene
    - Cloud security and AI risks
    - Secure handling of company and personal data

    Training records will be maintained and reviewed.

15. **Returning Equipment -** All old, unused, or damaged company laptops, tablets, and smartphones must be returned to the IT Department for secure disposal. Devices must not be disposed of, sold, or repurposed without formal clearance. This ensures that:

    - Sensitive data is securely erased
    - Software licences are reclaimed
    - Disposal complies with environmental and data protection requirements

    Contact IT if you believe a device is ready for return or needs secure disposal.

16. **Leaving or Changing Roles -** On leaving the company or changing roles, all equipment must be returned, and access rights will be reviewed. No employee may retain, copy, or share company data after departure.

17. **Policy Review -** This policy is reviewed annually or sooner if significant changes to threat landscape or company systems occur. All updates will be communicated to employees.



Jane Griffiths
Director
November 2025