

The National Piping Centre

The National Piping Centre Electronic Devices and Communications Policy

This policy applies to: Staff, Freelancers, Students, Visitors & Audiences.

This policy was reviewed on: 19/01/2026 by: Callum Stamper (Commercial Director)

This policy is due for review by: 31/01/2027

Electronic Devices and Communications Policy with GDPR Compliance

- Purpose and Scope:** This Electronic Devices and Communications Policy outlines the acceptable use of electronic devices and communication tools within The National Piping Centre. The policy applies to all employees, volunteers, contractors, and any other individuals granted access to The National Piping Centre premises, networks, or information systems.
- Authorized Devices:** a. Employees are permitted to use company-provided electronic devices (laptops, smartphones, tablets) for work-related purposes only. b. Personally owned devices may be allowed with prior approval from the IT department, provided they comply with security and compatibility standards.
- Internet and Network Usage:** a. Employees should use The National Piping Centre's network principally for business purposes, personal use is permitted but should be kept to a minimum. b. Accessing or downloading inappropriate, offensive, or illegal content is strictly prohibited. c. Employees should avoid excessive use of bandwidth for non-work-related activities.
- Email and Communication:** a. Company-provided email accounts are to be used for official communication. b. Confidential information should not be shared through unsecured communication channels. c. Use of external messaging platforms (e.g., WhatsApp, Telegram) for official business is not permitted unless approved by management.
- Data Security and GDPR Compliance:** a. Employees are responsible for safeguarding company data and ensuring compliance with the General Data Protection Regulation (GDPR). b. Personal devices used for work must adhere to GDPR guidelines and must not compromise the security of personal data. c. Employees should report any data breaches or incidents promptly to the Commercial Director.
- Bring Your Own Device (BYOD):** a. Where a BYOD arrangement is approved by the Commercial Director, employees must adhere to the BYOD rules and requirements outlined by the IT department. b. The organisation reserves the right to remotely wipe company data from personal devices in the event of loss or separation from the company.
- Social Media Usage:** a. Employees are expected to use social media responsibly and professionally. b. Employees must not share confidential or sensitive company

information or engage in activities that may violate GDPR regulations. If employees are in any way unsure whether information is confidential or sensitive they should seek approval from the Commercial Director.

8. **Monitoring and Enforcement:** a. The National Piping Centre reserves the right to monitor electronic devices, networks, and communications to ensure compliance with this policy and GDPR. b. Violations of this policy or GDPR may result in disciplinary action, up to and including termination of employment.
9. **Training and Awareness:** a. Employees will receive training on the proper use of electronic devices, communication tools, and GDPR compliance. b. Periodic reminders and updates on policy changes and GDPR regulations will be communicated to all employees.
10. **Policy Review:** a. This policy will be reviewed regularly and updated as needed to ensure ongoing GDPR compliance. b. Employees are encouraged to provide feedback to the Commercial Director to improve the effectiveness of this policy.

By adhering to this Electronic Devices and Communications Policy, employees contribute to maintaining a secure, GDPR-compliant, and productive work environment at The National Piping Centre.

The National Piping Centre

