**

Mobile Device Policy

|  |
| --- |
| Version History |
| Version No | Version Date | Author | Summary of Changes |
| 1.0 | 08/10/2019 | IMcG | First Issue |
| 1.01 | 07/12/2022 | MH | Changes to Section 6.1 BYOD referencing core ICT Policy and section 7.1 Mobile Devices and 6 digit pin codes. |
|  |  |  |  |

|  |
| --- |
| Approvals  |
| Name | Title | Date of Approval |
| Steve Darsey | Chairman | 27/01/2020 |
|  |  |  |
|  |  |  |

|  |
| --- |
| Distribution |
| Audience | Date of Issue | Version Number |
| All Staff | 27/01/2020 | 1.0 |
|  |  |  |

Table of Contents

1. Purpose
2. Scope
3. Definitions
4. Policy Statements
5. User Responsibility
6. Data Access and Storage
7. Device and Physical Security
8. Reporting Loss or Theft
9. Disciplinary Process
10. Deviations from Policy

#### **1.0 Purpose**

This document specifies the Erith Groups policy for the use, management and security of all Mobile Devices that may access or hold data owned by the Erith group. Laptops, Mobile Phones and Tablets, external storage, are all referred to as Mobile devices within this document.

#### **2.0 Scope**

2.1 This policy applies to all Erith Group issued Mobile Devices and personally owned Mobile Devices that are used to access Erith Group data and information, network or ICT facilities including, but not limited to, Ezone, Coins, Email, All Microsoft 0365 Applications, Teams, One drive, and Erith Group managed network drive storage.

2.2 This policy applies to all Users which includes staff, contractors, consultants, operating on behalf of the Erith Group, accessing the ICT systems.

2.3 Use of personally owned mobile devices to access and store Erith Group information, as well as a user’s own personal content, is commonly known as ‘bring your own device’ or BYOD. BYOD is supported within the Erith Group wireless network, for providing access to Email and Office 365 applications commonly known as O365 Apps, no access to internal resources is available via a BYOD as access to the Erith Group Domain will not be present.

2.4 All personally owned Mobile Devices connecting to the Erith Group WiFi network are treated as any other Internet connected unmanaged device, and users should take the same precautions in protecting data.

2.5 This policy recognises that personal Mobile Devices can be used to receive MFA alerts from O365 and Ezone login where required.

2.6 The Erith Group is under no obligation to modify its systems to allow Users to connect their personally owned Mobile Devices to them where such modification may be required.

2.7 The Erith Group ICT Department offers minimal Service Desk support for personally owned Mobile Devices, where this is necessary to enable Users to access Email and other O365 apps.

#### **3.0 Definitions**

‘*Erith Group*’ is a collection of companies that lie under the Erith umbrella. All these companies are referred to as the Erith Group. For the purposes of this document the companies within the Erith Group are known as; Erith Contractors Ltd, Erith Haulage Company Ltd, Erith Business Solutions Ltd, Erith Training Services Ltd, Swanton Consulting Ltd and Erith Plant Services Ltd.

Erith Group issued Mobile Device means any Mobile Device that has been purchased, is owned or leased by the Erith Group regardless of the source of funding.

Personally, owned Mobile Devices means any Mobile Device that is held personally by an individual in a private capacity.

For the purposes of clarification Mobile Devices include:

* Laptop computers
* Tablets
* Smart phones
* Portable external storage includes removable hard disks, CDs, DVDs, memory cards and USB pen drives

Confidential information consists of information which, if disclosed or made publicly available could damage commercial or financial interests, privacy, reputation or employability; could cause damage or distress to individuals; cause the Erith Group to not meet its legal obligations; or damage the Erith Group’s reputation. The definition of Confidential includes any information which is either labelled as ‘confidential’ or, if not labelled ‘confidential’, would nevertheless be reasonably regarded as confidential.

**4.0 Policy Statements**

To maintain the integrity and protection of the Erith Group’s ICT Network all equipment connected to the Erith Group’s network must comply with a set of minimum standards. Poorly configured, managed, or operated equipment may lead to serious degradation of network operation or a breach in network and systems integrity resulting in:

* Disruption to business-as-usual processes
* Disclosure of Erith Group information
* System or network compromise

4.1. The use of any Mobile Device to process and access Erith Group information creates risks including those relating to data protection, virus infection, and copyright infringement, unintentional or unlawful compromise of data and even loss or theft of device and/or data. The risks are increased, and are also more difficult to manage, when using personally owned Mobile Devices.

4.2. The Erith Group, and its staff, are required to process, and are committed to processing, all personal data in accordance with the Data Protection Act 1998 and the General Data Protection Regulation UK GDPR regardless of the device used to access the information. Users are required to keep Erith Group information and personal data secure. This applies equally to Erith Group information held on Erith Group systems and devices or accessed/held on personally owned Mobile Devices.

4.3. The Erith Group reserves the right to refuse to allow access to particular devices or software where it considers that there is a security or other risk to its information or ICT Network.

4.4. The Erith Group is the owner of all Erith Group information and the contents of Erith Group systems together with everything which is created on, transmitted to, received on, or printed from, or stored or recorded on each Mobile Device, in each case during the course of the Erith Group’s business or otherwise on the Erith Group’s behalf – irrespective of who owns that Mobile Device.

4.5. The Erith Group reserves the right to request access to inspect, or delete Erith Group information held on a personally owned Mobile Device to the extent permitted by law and for legitimate business purposes. Every effort will be made to ensure that the Erith Group does not access the private information of the individual.

4.6. Monitoring of The Erith Group’s ICT activity logs whether using Erith Group issued Mobile Devices or personally owned Mobile Devices, will be carried out in accordance with the ICT Acceptable Use Policy.

#### **5.0 User Responsibility**

Mobile Device Users are responsible for:

* The security of the Erith Group’s information and of the device on which the information is held.
* Storing Erith Group information on the Mobile Device only for so long as necessary
* Deleting Erith Group information from the Mobile Device when no longer required or sooner if required by the Erith Group to delete it.
* Ensuring, where possible, the device is up to date with the latest Operating System and anti-virus protection.
* Complying with this policy and the related employee policies.

**6.0 Data Access and Storage**

6.1. Use of any personally owned Mobile Device for business purposes must follow the guidelines laid out in section 6.23 of [05.01.01.02 ICT Policy](https://erithcontractorslimited.sharepoint.com/%3Aw%3A/s/InformationSecurity-ISO270012013/ET0ZDu-I2StDnp-_GWoisPIBN4ytsa4pnzMTKXygneALCg?e=8dYrME) and is at the User’s risk. The Erith Group is not liable for any losses, damages or liability arising out of such use, including but not limited to loss, corruption or misuse of any content or loss of access to or misuse of such personally owned Mobile Device, its software or its functionality.

6.2. When storing and/or processing confidential information on a mobile device, use of a Erith Group issued Mobile Device (i.e. laptop or tablet) should always be seen as the preferred mechanism. Storage on personally owned Mobile Devices can put confidential information at risk of compromise and may be subject to varied technical standards, support, as well as access by third parties.

6.3. Confidential information should be stored within and accessed from Erith Group information systems and Erith Group managed storage to ensure security of and appropriate secure access to the information.

6.4. Confidential information should not be stored or transferred to a cloud computing service other than the O365 Apps or any other approved service.

6.5. Only store the minimum amount of information necessary to carry out any required task on a mobile device. A temporary cache may be held on the device, therefore any confidential information should be deleted from the device as soon as the information is no longer required.

#### **7.0 Device and Physical Security**

7.1. Mobile Devices accessing Erith Group information must have a complex/strong password, minimum of a six digit passcode or PIN enabled to reduce opportunity for unauthorised access. Passwords, Passcodes and PINs must be kept secure. The device should be set to automatically lock if inactive for 5 minutes or less, or locked manually, where the feature is available biometrics can also be used to access mobile devices.

7.2. Mobile Devices should, where possible, have operating system and anti-virus updates enabled. “Jailbroken” or “rooted” devices or those mobile devices which have otherwise circumvented the installed operating system security requirements, making them vulnerable to compromise, are not permitted to connect to the Erith Group’s network and systems.

7.3. Erith Group Issued Mobile Devices are configured to use a comprehensive list of security measures prior delivery to the User, covering MDM, Antivirus, local firewalls and remote control and management software. All security measures must not be tampered with.

7.4. Erith Group issued Mobile Devices must not be left unattended whether on or off Erith Group premises and, where possible, must be physically locked away or secured.

7.5. The devices are Erith Group property and as such must be returned to ICT Department upon change of User or termination of employment. They must not be sold, given away or otherwise be disposed of by the user.

7.6. The ICT Department will manage the re-image before re-issue to another User (or secure erasure when disposing of devices at end of life, via our WEEE Waste Policy *8.3.2.1 ICT WEEE Waste Policy*.

7.7. If devices are not returned the matter will be passed to the Payroll Manager. The matter may also be passed to the Police for consideration of further action if required.

7.8. For personally owned Mobile Devices, employees must delete all Erith Group information from their device (on termination of their employment or, if the personally owned Mobile Device is repaired, exchanged, sold, given away or otherwise disposed of) and may be required to provide a written undertaking that this will be done. Without relieving employees of their obligation to delete all Erith Group information, the Erith Group’s rights under paragraph 4.5 above apply, including after termination of employment.

#### **8.0 Reporting Loss or Theft**

8.1. In the event of loss or theft of any Mobile Device irrespective of whether it is a Erith Group issued Mobile Device or a personally owned Mobile Device (used to access Erith Group information, Network or ICT systems), the User must act promptly to minimise the risk of compromise to Erith Group information by immediately:

* Changing their Erith Group network log in password and notifying ICT Helpdesk of incident circumstances.
* Changing any other passwords that may have been used on the device.
* Reporting theft of device to the Police, for the crime reference number.
* Reporting loss or theft of mobile device to the ICT Department so that to the mobile network carrier directly.

8.2. Appropriate steps will be taken to ensure that Erith Group information on or accessible from the Mobile Device is secured, including remote wiping of the Mobile Device, where possible. The remote wipe will destroy all Erith Group data on the Mobile Device. Although it is not intended to wipe other data that is personal in nature (such as photographs or personal files or emails), it may not be possible to distinguish such information from Erith Group data in all circumstances. It is the responsibility of the user, therefore, to regularly backup all personal data stored on the Mobile Device. The Erith Group does not guarantee the availability of data stored on a mobile device in the event of loss, theft or destruction, although mailbox data will remain intact.

**9.0 Disciplinary Process**

The Erith Group reserves the right to audit compliance with the policy from time to time. Any disciplinary action, arising from breach of this policy, shall be taken in accordance with the Erith Groups Disciplinary Policy. Disciplinary action may ultimately lead to dismissal.

#### **10.0 Deviations from Policy**

Unless specifically approved, any deviation from this policy is strictly prohibited. Any deviation from or non-compliance with this policy shall need to be reported to and approved by the ICT Director.

Signed for and on behalf of

The Erith Group



Steven Darsey

Chairman