**

Acceptable Use Policy

|  |
| --- |
| Version History |
| Version No | Version Date | Author | Summary of Changes |
| 1.0 | 11-11-17 | MH | First Issue |
| 1.1 | 18-11-19 | IMcG | Added new definitions and updated the references to linked documents. |
| 1.2 | 26-11-19 | IMcG | Section 5.4 Acceptable use of assets  |
| 1.3 | 04-12-19 | MH | Telephone System changes |
| 1.4 | 09-12-19 | IMcG | Security assets off-premises |
| 1.5 | 22-05-20 | IMcG | Amended copyright & computer misuse act – reviewed formatting (4.4.18) |
| 1.6 | 21-03-22 | IMcG | Changes to the scope of social media use. |

|  |
| --- |
| Approvals  |
| Name | Title | Date of Approval |
| Matt Harper | IT Director | 11/11/2017 |
| Matt Harper | IT Director | 18/11/2019 |
| Matt Harper | IT Director | 26-11-2019 |
| Steve Darsey | Chairman  | 27/01/2020 |
| Matt Harper | IT Director | 22/05/2020 |
| Matt Harper | IT Director | 21/03/2022 |

|  |
| --- |
| Distribution |
| Audience | Date of Issue | Version Number |
| All Staff | 11/11/2017 | 1.0 |
| All Staff | 27/01/2020 | 1.4 |
| All Staff | 22/05/2020 | 1.5 |
| All Staff | 21/03/2022 | 1.6 |

Table of Contents

1. Purpose
2. Scope
3. Definitions
4. Policy Statements
5. Compliance measurement
6. Exceptions
7. Disciplinary

#### **1.0 Purpose**

The purpose of this policy is to outline the acceptable use of computer equipment at The Erith Group. These rules are in place to protect the employee and The Erith Group. Inappropriate use exposes The Erith Group to risks including virus attacks, compromise of network systems and services, and legal issues.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, CRM, ERP and FTP, are the property of The Erith Group. These systems are to be used for business purposes in serving the interests of the company, and of our clients and customers in the course of normal operations.

Effective security is a team effort involving the participation and support of every one The Erith Group’s employees who deal with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

 **2.0 Scope**This policy applies to the use of Assets, information, electronic and computing devices, and network resources to conduct The Erith Group business or interact with internal networks and business systems, whether owned or leased by The Erith Group, the employee, or a third party.

All employees, contractors, consultants, temporary, and other workers at The Erith Group and its subsidiaries are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with The Erith Group’s policies and standards, and local laws and regulation.

This policy applies to employees, contractors, consultants, temporaries, and other workers at The Erith Group, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by The Erith Group.

#### **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.

Information Systems – includes all servers and clients, Laptops, mobile devices, removable storage media, network infrastructure, system and application software, and other computer subsystems and components which are owned or used by the Erith Group or which are under the Erith Group’s responsibility. The use of an Information System also includes the use of all internal or external services, such as Internet access, e-mail, etc.

Information Assets – in the context of this Policy, the term Information Assets is applied to Information Systems and other information/data irrespective of form, i.e. electronic information and paper documents.

Approved Users – refers to all Employees of the Erith Group. which includes contractors, consultants, operating on behalf of the Erith Group, accessing the Erith Group ICT systems

COR – Confirmation of Receipt, this is a signed document by the approved user, confirming that they agree to the Erith Group’s ICT Security policies.

**4.0 Policy Statements**

## General Use and Ownership

* + 1. The Erith Group proprietary information stored on electronic and computing devices whether owned or leased by The Erith Group, the employee or a third party, remains the sole property of The Erith Group. You must ensure through legal or technical means that proprietary information is protected in accordance with the UK GDPR *Data Protection Standard.*
		2. You have a responsibility to promptly report the theft, loss or unauthorised disclosure of The Erith Group’s proprietary information.
		3. You may access, use or share The Erith Group’s proprietary information only to the extent it is authorised and necessary to fulfill your assigned job duties.
		4. Employees are responsible for exercising good judgment regarding the reasonability of personal use of The Erith Group’s proprietary information.
		5. For security and network maintenance purposes, authorised individuals within The Erith Group may monitor equipment, systems and network traffic at any time.
		6. The Erith Group reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

## Security and Proprietary Information

* + 1. All mobile and computing devices that connect to the internal network must comply with the *9.1.2.1 ICT - Minimum Access Policy*.
		2. System level and user level passwords must comply with the *9.3.1 ICT - Password Policy*. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.
		3. You must lock the screen or log off immediately in order before leaving the device unattended, and the unlock mechanism must require you to provide your Windows Logon Password
		4. Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware.
		5. Wherever vendors allow, Multi Factor Authentication will be employed to maintain Information Security

## Unacceptable Use

## The following activities are, in general, prohibited. Employees may be exempted from these restrictions during their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services)

## Under no circumstances is an employee of The Erith Group authorised to engage in any activity that is illegal under domestic or international law while utilising Erith Group owned resources or assets.

## The lists below are by no means exhaustive but attempt to provide a framework for activities which fall into the category of unacceptable use.

* 1. **System and Network Activities**

The following activities are strictly prohibited, with no exceptions:

* + 1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by The Erith Group.
		2. Unauthorised copying of copyrighted material including, but not limited to, digitisation and distribution of photographs from magazines, books or other copyrighted sources and the installation of any copyrighted software including software piracy, either by illegal download or illegal distribution, use of software without the relevant software license, theft of intellectual property such as designs for 3D printers or text/written work, using/downloading images without permission of the copyright holder, illegal download of video and audio files.
		3. Accessing data, a server or an account for any purpose other than conducting The Erith Group business, even if you have authorised access, is prohibited.
		4. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
		5. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
		6. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
		7. Using an Erith Group computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
		8. Making fraudulent offers of products, items, or services originating from any Erith Group account.
		9. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
		10. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorised to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
		11. Port scanning or security scanning is expressly forbidden.
		12. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
		13. Circumventing user authentication or security of any host, network or account.
		14. Introducing honeypots, honeynets, or similar technology on The Erith Group network.
		15. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
		16. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
		17. Providing information about, or lists of, The Erith Group employees to parties outside The Erith Group.
		18. Unlawfully gaining access to computer programs covering, unauthorised access to computer material, unauthorised access with intent to commit or facilitate commission of further offences and unauthorised acts with intent to impair, or with recklessness as to impairing, operation of computer.
		19. Adapt, supply or obtain articles for use in unlawfully gaining access to computer material or impairing the operation of a computer.
	1. **Email and Communication Activities**
		1. When using company resources to access and use the Internet, users must realise they represent the company. Questions may be addressed to the ICT Department helpdesk@erith.com.
		2. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam) is strictly prohibited.
		3. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
		4. Unauthorised use, or forging, of email header information.
		5. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
		6. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
		7. Use of unsolicited email originating from within The Erith Group's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by The Erith Group or connected via The Erith Group's network.
	2. **Blogging and Social Media**
		1. Blogging by employees about any Erith Group company, whether using The Erith Group’s property and systems or personal computer systems, is STRICTLY PROHIBITED.
		2. Limited and occasional use of The Erith Group’s systems to engage in personal blogging is acceptable, if it is does not mention any Erith Group company or contain any imagery which depicts the Erith Group’s assets or can identify the group specifically.
		3. The Erith Group’s Confidential Information policy also applies to blogging. As such, Employees are prohibited from revealing any Erith Group confidential or proprietary information, trade secrets or any other material covered by Erith Group Confidential Information policy when engaged in blogging.
		4. Employees shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of The Erith Group and/or any of its employees. Employees are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments.
		5. Employees may also not attribute personal statements, opinions or beliefs to The Erith Group when engaged in blogging. If an employee is expressing his or her beliefs and/or opinions in blogs, the employee may not, expressly or implicitly, represent themselves as an employee or representative of The Erith Group. Employees assume any and all risk associated with blogging.
		6. Apart from following all laws pertaining to the handling and disclosure of copyrighted or export-controlled materials, The Erith Group’s trademarks, logos and any other Erith Group intellectual property may also not be used in connection with any blogging activity.
	3. **Acceptable use of Asset**
		1. Use of these assets for personal activities (provided that it does not infringe any of the regulations, and does not interfere with others’ valid use) is permitted, but should be kept to a minimum.
		2. Personal use is subject to the following limitations:
* It is only available for use by approved users.
* The level of use must be reasonable and not detrimental to the Erith Group.
* Priority must be given to use of resources for the main purpose for which they are provided.
* Personal use must not be for a commercial purpose.
* Personal use must not be of a nature that competes with the Erith Group.
* Personal use must not be connected to any use or application that conflicts with the Erith Group’s rules, regulations, policies, or procedures, including this policy.
* It is a privilege that may be withdrawn at any point.
	+ 1. You must not do anything to jeopardise the integrity of the Information Systems by, for example, doing any of the following without approval.
* Damaging, reconfiguring Erith Group Assets including, Laptops Desktops, Printers, scanners and monitors, servers Mobile Devices etc.
* Loading software on to the Erith Group equipment other than in approved circumstances.
* Reconfiguring or connecting equipment to the network other than by approved methods.
* Setting up servers or services on the network.
* Deliberately or recklessly introducing malware.
* Attempting to disrupt or circumvent any Information Security controls set out by the ICT Department.

* 1. **Information Assets**
		1. If you handle internal, restricted or confidential information, you must take all reasonable steps to safeguard it and must observe the Erith Groups;
* 5.1.1.01 ICT - Information Security Policy
* 5.1.1.02 ICT - Information Technology Policy
* 5.1.1.04 ICT - Data Protection Act Policy
* 10.1.1 ICT - Cryptography Control Policy.
	+ 1. You must not attempt to access, delete, modify, or disclose Information assets belonging to other people without their permission, unless it is obvious that they intend others to do this.
		2. It is prohibitedto use information assets in a manner that unnecessarily takes up capacity, wastes staff effort or other IT resources, weakens the performance of the information system or poses a security threat.
		3. It is also prohibitedto:
* Create or transmit material with the intent to defraud.
* Create or transmit defamatory material
* Create or transmit material such that this infringes the copyright of another person or the Erith Group.
* Disrupt the work of other users, deny them access to services, or corrupt or destroy their data.
	+ 1. You should not consume excessive bandwidth by uploading or downloading more material (particularly video) than is necessary.
		2. Do not waste paper by printing more than is needed, or by printing single-sided when double-sided would suffice.
		3. Do not waste electricity by leaving equipment needlessly switched on.
		4. Upon termination of an employment contract or other contract on the basis of which various equipment, software or information in electronic or paper form is used, the Employee must return all such information assets and physical assets to his/her line manager or the asset owner in accordance to the COR that was signed on receipt of the asset.
		5. When using an asset off premises the asset owner must ensure that the asset is used and stored safely and within the correct environmental conditions.
		6. While the asset is being used off premise the asset owner must ensure that the asset is not stolen damaged or misused in any way.
		7. If the assets are being used in a Teleworking environment then they must be done so in accordance with the *6.2.2 ICT - Teleworking Policy*.
		8. Where available the facility to remote control an asset will be enabled to wipe remotely or locate the asset in the event of theft or loss.
	1. **Use of Telephones**
		1. Any prestige that attaches to the Erith Group’s name can be enhanced or damaged using the telephone or other communication tools. Incoming calls must always be answered promptly and courteously. In the event that the employee for whom the call is intended is not available and the caller elects to leave a message, this is to be written down carefully and passed to the employee concerned at the earliest available opportunity.
		2. Although employees are not expected to use the telephone for private calls, the Directors recognise that sometimes the private business of employees can only be transacted during working hours. However, it must be understood that this privilege involves obligations and private business should be transacted on the Erith Group’s telephone/ICT system only when no other means are available. Abuse of this privilege may give rise to disciplinary action under the Erith Group’s disciplinary procedure

#### **5.0 Compliance Measurement**

The ICT Director will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the Operations Board.

**6.0 Exceptions**

Any exception to the policy must be approved by the ICT Director in advance.

**7.0 Disciplinary Process**

An employee found to be in violation this policy may be subject to disciplinary action, up to and including termination of employment.

# 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.

Signed for and on behalf of

The Erith Group



Steven Darsey

Chairman