P4 S1 Information & Communication Technology (ICT) Acceptable Usage Policy and Procedures

SCOPE

This policy applies to any person authorised to have access to Forus Training information systems. This includes, but is not limited to, Forus Training employees, contractors to Forus Training and consultants engaged by Forus Training hereafter collectively referred to as users for the purpose of this policy.

This policy applies to all electronic communications systems provided by Forus Training including, but not limited to internet, intranet, email, social media accounts, personal computers and laptops, digital cameras, PDAs (personal digital assistants), telecommunication systems and devices. It is the responsibility of both management and staff of Forus Training to ensure that all such tools are used in accordance with this policy.

All users are expected to use common sense and to conduct themselves in a manner that is appropriate to the execution of duties in the workplace. Breaches of this policy may result in personal liability of users and/or vicarious liability on behalf of Forus Training under many enactments including, but not limited to, the following:

- Employment Equality Acts, 1998,
- Equal Status Act, 2000 and 2012,
- Data Protection Legislation, (Data Protection Act 2018),
- Freedom of Information Act 2014,
- General Data Protection Regulations GDPR,
- The Education and Training Boards Act, 2013,
- The Companies Acts 1963 - 2001,
- Copyright and Related Rights Act 2000, 2004 and 2007,
- Child Trafficking and Pornography Act 1990 1998 and 2004.

Other documentation that is relevant to this policy includes Forus Training policies on:

- Social Media,
- Data Protection,
- Mobile Phone,
- Grievance Procedure,
- Discipline Procedures,
- Dignity and Respect at Work,
- Equality and Diversity,
- Harassment and Sexual Harassment Prevention,
- Bullying in the workplace Prevention,

- Protected Disclosures,
- Bring Your Own Device (BYOD) (in development).

GENERAL COMPUTER USAGE REGULATIONS AND GUIDELINES

Contents
All electronic content created or received using equipment or services provided by Forus Training will be regarded as the property of Forus Training.

Equipment and Resources
All equipment provided by Forus Training for use by staff remains the property of Forus Training. Employees must not remove any such equipment including but not limited to computers, laptops, mobile telephones, etc. from Forus Training's premises without prior authorisation from the line manager. If equipment is removed it must be kept in a secure environment by the user.

It is the user's responsibility to be informed of the correct operating procedures for the resources or products used. A user who is uncertain as to the correct procedure in any situation should obtain clarification before proceeding.

Users must not engage in conduct that interferes with other's use of shared computing resources and/or the activities of other users.

Security and Passwords
Users must not utilise any other person's access rights or attempt to gain access to resources or data. In exceptional circumstances where access is required, it must be requested in writing by the Managing Director to the IT Department. Users must not attempt to bypass or probe any security mechanisms governing access to the computer systems.

No user may misrepresent himself / herself as another individual. This includes using another user's username and password.

Passwords must remain confidential to each user and must not be relayed to any other person. The IT Department may provide the option to alter any passwords as necessary. Passwords should be changed on a regular basis and should be of sufficient

strength to deter guessing or cracking. It is recommended that passwords should be a minimum of 8 characters and include a mixture of letters (upper and lower case) and numbers. Each user carries sole responsibility for security access to his/her computer, laptop or any other electronic device.

Each user must shut down his/her own computer on completion of work. In order to protect sensitive information, users should lock and password protect their PC when they are absent from their desks. Users who use devices off-site must ensure regular connection to the ETB network in order to keep the device updated.

Software Ownership

All software which is provided by Forus Training to a user is licensed and owned by Forus Training and may not be downloaded, stored elsewhere or transferred to another individual by any Forus Training user.

Under no circumstances should software be downloaded from the Internet or installed from any other source and used on Forus Training's equipment without the prior permission of the IT Department/Head of IT. Any breach of these requirements may result in disciplinary action.

Confidentiality

Users must maintain confidentiality while carrying out their duties and while on Forus Training business. Users must ensure that callers to offices are unable to view personal/sensitive information displayed on computer monitors.

Users must not register with an electronic service over the internet without prior consultation with the IT Department. This is to avoid release of confidential Forus Training information to third parties and to avoid interference with the communication systems.

Privacy

It should be understood that Forus Training does not provide users with a guarantee of, or to the right to privacy or confidentiality in connection with the use of any technology and users should have no expectation of privacy in the use of Forus Training IT resources.

Monitoring Policy

Forus Training reserves the right and intent to monitor, intercept or download email content and internet usage and files to ensure technology is being used properly and to protect Forus Training and its employees from liability. This does not constitute infringement of any individual rights to personal privacy under the Data Protection legislation.

Monitoring may be carried out on all Electronic Data including all Web site, Desktop, Laptop and Server content. This list is not exhaustive. Monitoring technology and policies may change over time. In addition, Forus Training may monitor devices for inappropriate images and content.

Legal Implications of Storing Electronic Data
All information held in electronic format is subject to legislative requirements, as is information held in paper format. These requirements include, but are not limited to, Copyright, Data Protection and Freedom of Information Legislation and the liabilities which may result from breaches of such legislation.

Personal information should contain only information relevant to the individual and to the purpose for which it is being stored. Personal Data obtained and stored on Forus Training systems or devices must not be used for any other purpose other than the sound legal basis identified for collection and processing. Please refer to Forus Training's Data Protection Policy for further information. This data must be maintained in an accurate format and kept secure at all times. The data must be altered if the user becomes aware of inaccuracies subject to authorisation by line management.

It is an offence to alter or falsify documents in an electronic format or paper / hard copy format. Care must be taken when forwarding or sending information which has been received from a third party or which is specific to another organisation.

Users should be aware that merely deleting information may not remove it from the system and that deleted material may still be reviewed by Forus Training and / or disclosed to third parties.

Material of obscene or offensive nature
Users are subject to legislation regulating the use of Forus Training's IT/Communications resources. Users may not store, download, upload, circulate or otherwise distribute material containing:

Any derogatory comment regarding gender, marital status, family status, sexual orientation, religious or political belief, age, disability, race or membership of the travelling community or other categories pursuant to applicable law.

- Any material of a pornographic nature,
- Any material of a paedophilic nature,
- Material containing offensive or foul language,
- Any content prohibited by law.

If an employee receives any offensive, unpleasant, harassing or intimidating messages via email or other computer sources the employee should bring it to the attention of their manager.

Security protection
Threats including, but not limited to viruses, spyware, malware, ransomware etc. can enter an organisation a number of different ways including:

- Unscanned digital storage media (e.g. CDs, DVDs, floppy disks, USB memory sticks) being brought into the organisation,
- Emails or attachments,
- Downloaded data from the Internet.

Individuals using electronic media including but not limited to USB, SD Cards, CD's and other storage devices must ensure they scan the media before connecting it to a Forus Training device. It is the personal responsibility of each individual to take precautions to ensure that viruses are not introduced into any Forus Training resources or system with which they come into contact.

No user may interfere with or disable the security software installed on their device. Any virus, virus error messages or security incidents must be reported promptly on Forus Training's Helpdesk portal https://forustraining.ie/
Do not forward a virus email warning to anybody else.

Such warnings are usually hoaxes and are designed to persuade users to delete system files on their device; forwarding such an email could make Forus Training liable for damage to computer systems outside Forus Training.

E-MAIL

Employees have an Forus Training email account to facilitate the sending and receiving of business messages between Staff and between Forus Training and third parties. Such communications should be carried out using the user's Forus Training email address only. While email brings many benefits to Forus Training in terms of its communications internally and externally, it also brings risks to the organisation, particularly where employees use it outside of their Forus Training roles.

Every employee has a responsibility to maintain Forus Training's image, to use electronic resources in a productive manner and to avoid placing Forus Training at risk for legal liability based on their use. It

should be remembered that the contents of email are considered as official records for the purpose of legislation such as Freedom of Information Act, National Archives Act and GDPR.

Risks Associated with Email

- Messages can carry viruses that may be seriously damaging to Forus Training's systems,
- E-Mail attachments may belong to others and there may be copyright implications in sending or receiving them without permission,
- It has become increasingly easy for messages to go to persons other than the intended recipient and if confidential or commercially sensitive, this could be breaching Forus Training's security, confidentiality, or the privacy rights of a data subject. Please remember to password protect attachments containing personal data,
- E-mail is speedy and, as such, messages written in haste or written carelessly are sent instantly and without the opportunity to check or rephrase. This could give rise to legal liability on the part of Forus Training,
- An email message may legally bind Forus Training contractually in certain instances without the proper authority being obtained internally,
- E-mails should be regarded as potentially public information which carries a heightened risk of legal liability for the sender, the recipient and the organisations for which they work.

Rules for Email use

The content of any email must be in a similar style to that of any written communication such as a letter or report as they may have the same legal standing. It is important that emails are treated in the same manner as any other written form of communication in terms of punctuation, accuracy, brevity and confidentiality. Similarly, any written, stored or forwarded and disseminated information must adhere to legislation and Forus Training policies.

In order to avoid or reduce the risks inherent in the use of email within Forus Training the following rules must be complied with:

- Forus Training's email disclaimer or a link to the same must appear at the end of every email sent from your Forus Training's address to an external address,

- Forus Training's name and logo is included in the address of all staff members and is visible to all mail recipients. This reflects on the image and reputation of the organisation, therefore, email messages must be appropriate and professional,
- Correct spelling and punctuation should be maintained in all communications.
- Forus Training email is provided for business purposes,
- Occasional and reasonable personal use of email is permitted provided that this does not interfere with the performance, work duties, responsibilities and customer service of Forus Training. Email may not be used in support of any business other than Forus Training and must comply with the stipulations contained in this policy,
- An email should be regarded as a written formal letter, the recipients of which may be much more numerous than the sender intended. Therefore, any defamatory or careless remarks can have serious consequences, as can any indirect innuendo. The use of indecent, obscene, sexist, racist, harassing or other appropriate remarks whether in written form, cartoon form or otherwise is forbidden,
- E-mails must not contain matters which may discriminate on grounds of gender, marital status, family status, age, race, religion, sexual orientation, disability or membership of the Traveller community,
- Emails must not contain any inappropriate or lewd content or content likely to cause offence,
- Distribution lists may only be used in connection with Forus Training business,
- Documents prepared internally for the public or for clients may be attached via e- mail. However, emailing excerpts from reports other than our own may be in breach of copyright and the author's consent should be obtained particularly where the excerpt is taken out of its original context. Information received from a customer should not be released to another customer without prior consent of the original sender. If in doubt consult your manager,
- Do not subscribe to electronic services or other contracts on behalf of Forus Training unless you have express approval to do so from your manager and/or the IT Department,
- If a user receives any offensive, unpleasant, discriminatory, harassing or intimidating messages via the email system they must immediately inform their manager,
- Chain mails or unsuitable information must not be forwarded internally or externally,
- Forus Training reserves and intends to exercise the right to review, audit, intercept, access and disclose all messages created, received or sent over the electronic mail system for any purpose or where it deems necessary,
- Notwithstanding Forus Training's right to retrieve and read any electronic mail messages, such messages should be treated as confidential by other employees and accessed only by the intended recipient. Employees are not authorised to retrieve or read any email messages that are not sent to them. However, the confidentiality of any message should not be assumed. Even when a message is erased it is still possible to retrieve and read that message,

- If a user registers with a site or a service in the name of Forus Training the resulting spamming of information may tie up the communications system. Users must not register with an electronic service or website without prior permission from their Manager and from the Head of IT, to avoid the release of confidential Forus Training information to third parties and to avoid interference with the communications systems,
- Users should take the time to review each email before sending to ensure the message is clear and is relaying the right tone (Try reading it out loud). It may be useful to ask yourself if you are happy that the content of the email could be displayed on a public notice board. If not, consider rephrasing or using other means of communication,
- Users should avoid sending email text in capitals. IF YOU WRITE IN CAPITALS IT SEEMS AS IF YOU ARE SHOUTING. This can be frustrating and may trigger an unwanted response from the recipient,
- 'Reply All' should be used only if it is necessary for the message to be seen by each person who received the original message. In most cases, replying to the sender alone is sufficient,
- When forwarding an email please check if it is necessary to forward the whole thread on the email. There may be some information or personal data in the thread of the email that does not need to be shared,
- If users are out of the centre/office/home office and unable to respond to email for extended periods, they must set up an auto-reply message for incoming emails that notifies senders of plans for responding to their emails and/or an alternative contact person,
- If the message is important, users should obtain confirmation that the intended recipient(s) received your email by using the "Request a Read Receipt" option on the Tools menu. However, this function should not be used to automatically request a receipt for every email sent, it should be used only as required,
- Messages should be regularly reviewed and those that have been actioned and are no longer needed should be deleted, in order to ensure that disk space is managed efficiently,
- Users should be aware of the risk of viruses being sent in email messages or attachments. Users should be vigilant for unsolicited or unexpected emails and never open attachments or click on links contained in emails from addresses or people they do not recognise.

THE INTERNET/INTRANET

Forus Training provides a managed network across all its and centres. Access to the network is provided to staff as necessary solely for the purpose of conducting Forus Training's business. All information and uploaded content on the intranet is the property of the Forus Training.

Rules for Internet use

- Forus Training Internet connections are intended for activities related to Forus Training's activities,
- Internet usage may be monitored on a systematic basis and as deemed necessary by the IT Department,
- Unauthorised downloading of any software programmes or other material is forbidden,
- It is a disciplinary offence to access, download, save, circulate or transmit any racist, defamatory or other inappropriate materials or materials that may discriminate on the grounds of gender, marital status, family status, age, race, religion, sexual orientation, disability or membership of the Traveller community. This rule will be strictly enforced and is viewed very seriously with potential criminal liabilities arising therefrom,
- It is a disciplinary offence to access, download, save, circulate or transmit any indecent, obscene, child pornographic or adult pornographic material,
- If a user downloads pornographic images within view of a colleague or forwards those images to a colleague, this may result in harassment or sexual harassment by offended parties. Such incidents should be reported to Forus Training. Apart from any potential offence caused and the inappropriateness of such activity, Forus Training may be vicariously liable for any claims arising from such behaviour,
- Because of the serious criminal implications of accessing child pornography, any user found to be accessing such information may be summarily dismissed and the matter referred to An Garda Síochána. Furthermore, should an employee be prosecuted under the Child Trafficking and Pornography Act, 1998, by engaging in such activities outside the remit of the workplace, Forus Training may find it fitting to invoke disciplinary action,
- The Internet must not be used to pay for, advertise, participate in or otherwise support unauthorised or illegal activities,
- The Internet must not be used to provide lists or information about the organisation to others and/or to send classified information without prior written approval.

Rules for Network Use

- Employees may not tamper with any network equipment/cabling unless instructed by a member of the IT department,
- Employees are strictly prohibited from installing/connecting any additional network equipment e.g. wireless access points, wireless routers, 3G dongles, etc. without prior approval from the IT department.

LAPTOPS AND REMOTE DEVICES SUPPLIED BY FORUS TRAINING

The rules applying to use of the Internet and email messaging systems apply also to any laptops, tablets, mobile phones or other electronic devices in use by staff members and supplied by Forus Training.

All devices should be password and/or PIN protected to prevent unauthorised use of the device and unauthorised access to information held on the device.

Personal, sensitive or confidential data should not be stored on Forus Training laptops or other portable devices, however where this is unavoidable, the device should be equipped with encryption software. Security software must be installed and kept up-to-date on all portable devices. Please see Appendix 1 for instructions on encrypting mobile phones.

Authorisation must be obtained from the Manager to remove such equipment/devices from ETB premises. All such equipment will be subject to the same monitoring procedure as that which is retained on-site.

TELEPHONE USAGE

Access to Forus Training telephones is intended for Forus Training purposes only. While reasonable making and taking personal calls is not strictly prohibited, staff are encouraged to keep this to a minimum level. Forus Training reserves the right to monitor the use of the telephone system.

Some mobile phones are provided to staff members for Forus Training business. Personal calls from such phones are permitted but the calls must be paid for by the staff member. For more specific information, see Forus Training's Mobile Phone Policy.

During office hours, the taking and/or making of calls on personal mobiles is not strictly prohibited however, staff are encouraged to keep such calls to a minimum. The making and receiving of personal calls or texts, particularly during the course of classes or meetings, is deemed inappropriate.

OTHER ELECTRONIC TOOLS

Other electronic equipment (e.g. fax machines, photocopiers etc.) remain the property of Forus Training and as such must be treated with care and used only for Forus Training purposes. Abuse of equipment for personal use or gain may result in the use of the disciplinary procedures and in disciplinary action.

PLAGIARISM

Users should not plagiarise (or use as their own, without citing the original creator) content, including words or images from the Internet. Users should not misrepresent themselves as the author or creator of something found on-line. Research conducted via the Internet should be appropriately cited, giving credit to the original author.

SOCIAL MEDIA

Forus Training recognises the presence and value of social media tools which can facilitate communication, learning and collaboration. When using these tools, users are expected to communicate with the same appropriate and professional conduct online as offline.

Users should consider rules governing copyright, intellectual property and confidentiality before posting to social media.

Users should be mindful of their privacy settings and postings on personal social platforms. Employees should note that the use of social media in a work setting is subject to the same guidelines and rules as previously outlined in this policy. For more specific information, see Forus Training's Social Media Policy.

REMOVABLE MEDIA

No non-Forus Training approved removable media such as CD, DVD, USB drive or SD cards etc. that contain data or files may be used without consulting with the IT Department.

ENCRYPTION

All personal data stored on Forus Training mobile devices must be protected by encryption software. It is the responsibility of the staff member to ensure that the data is encrypted and the encryption software is up to date. This responsibility includes data stored on personal devices.

Only encryption software recommended by Forus Training should be used. For guidance on enabling encryption on mobile devices see Appendix 1.

INFRINGEMENTS OF POLICY

Failure to comply with the policy and guidelines outlined above may result in:

- The withdrawal of email and Internet facilities from the Section, Staff or users involved,
- Initiation of disciplinary procedures and disciplinary action, up and to including dismissal,
- Serious breaches of the policy may result in initiation of criminal or civil proceedings.

TRAINING AND SUPPORT

Training and support will be provided to users as and when required in order to assist in the appropriate use of ICT resources across Forus Training services.

Appendix 1

How to encrypt and password protect your Android phone;

1. To setup a PIN on your phone under Settings > Security > Screen Lock and set your PIN,
2. To set up encryption, plug your phone into a power source. The process can take an hour or more depending on how much data requires encrypting,
3. Ensure that you have backed-up all your important data,
4. Go to Settings -> Lock Screen -> Screen Lock -> [enter current password] -> Password and create a password that is at least 4 characters long, and contains at least 1 number. Note there is a limit of 16 characters. If you do not perform this step first, you will be sent back to do it when you start to encrypt your device,
5. Go to Settings -> System -> Security -> Encrypt device,
6. Select “Encrypt Phone” to confirm encryption. You will be asked once more to confirm your password,
7. Once completed, you need to enter your master password each time you reboot your phone.

How to encrypt and password protect your iPhone;

1. Go to the Settings on your phone,
2. Go to Touch ID & Passcode,
3. Select the Turn Passcode On option if it is not already. From there, you will be able to set either a strong six-digit or longer numerical passcode, or alphanumeric password,
4. Set a strong passcode. If you enter a code like "123456" it will warn you that it is easy to guess,
5. At this screen, selecting Passcode options will allow you to set a longer numerical passcode by choosing Custom Numeric Code. This offers the benefit of only giving you numbers to press on the lock screen
6. You can also set a Custom Alphanumeric Code, which significantly improves your device's security. According to Apple, setting a six-digit alphanumeric passcode with a combination of lower-case letters and numbers would take about five years to break if every combination was tried,
7. Once your passcode is set, you will return back to the Settings menu. Scroll down to the bottom of the page, you should see: "Data protection is enabled." That means your device is now encrypted.

The instructions above may vary depending on your device manufacturer/model. Please consult your device documentation for more information if required.

How to encrypt and password protect your Windows 10 Mobile;

Device encryption is an option that comes disable by default, but you can easily enable the feature using the following steps:

1. While in the Start screen, swipe left to bring All apps, then search for and open the Settings app, and tap on System,
2. Next, tap on Device encryption,
3. Finally, make sure to slide the Device encryption pill switch to the On position to enable the feature,
4. Important Note: A password PIN must be in place to enable the feature if your mobile device doesn't have one when trying to enable Device encryption, you will be automatically redirected to the Sign-in options settings page to create a PIN. Then you would just tap the Add button, under the PIN section, and follow the on-screen wizard to create a new PIN. After the PIN password is created, you can go back to Device encryption settings to verify that the feature has been enabled,
5. While the feature should work as expected, Windows Phone 8.1 used to display an "encrypted" label in the phone storage settings, and Windows 10 Mobile doesn't provide such visual confirmation in the storage settings. The only way to verify your device is being encrypted is by making sure the "Device encryption" is turned on in the Settings app,
6. It's important to point out that while encryption is enabled on your mobile device, the operating system and your data stored in the local storage will be encrypted, but device encryption will not encrypt data that you stored on an SD card. As such, it's highly recommended that you not save sensitive data on a removable storage, as anyone could easily remove the storage and have unrestricted access to that data from any computer,
7. Furthermore, you need to be careful when to choose to enable this feature, as it's possible that encrypting your device may cause some issues, such as problems with emails not synchronizing with your phone.