gretb

Bord Oideachais agus Oiliúna
na Gaillimhe agus Ros Comáin
Galway and Roscommon
Education and Training Board

GALWAY AND ROSCOMMON ETB
INFORMATION TECHNOLOGY
ACCEPTABLE USAGE POLICY

Document Information and Revision History

Revision Number	001
Approval Date	11 June 2019
Next Revision Date	June 2021
Document Developed by	IT Department
Document Approved by	Board of GRETB
Responsibility for implementation	All GRETB IT Systems Users
Responsibility for Audit and Review	Director of OSD

Version 1.0

This policy may be updated at any time (without notice) to ensure changes to GRETB's organisation structure and/or business practices are properly reflected in the policy. Please ensure you check GRETB intranet for the most up to date version of this policy

1.0 Purpose

Galway and Roscommon ETB is committed to the correct and proper use of its Information Technology (I.T.) resources in support of its administrative and teaching and learning functions.

The inappropriate use of information technology (I.T.) resources could expose GRETB to risks including virus and malicious software attacks, theft and unauthorised disclosure of information, disruption of network systems and services or litigation. The purpose of this policy is to provide GRETB staff and other users of its I.T. resources with clear guidance on the appropriate, safe and legal way in which they can make use of the organisations I.T. resources.

This policy is mandatory and by accessing any I.T. resources which are owned or leased by GRETB, users are agreeing to abide by the terms of this policy.

2.0 Scope

This policy represents GRETB's position and takes precedence over all other relevant policies which are developed at a local level. The policy applies to:

- All Information Technology (I.T.) resources provided by GRETB;
- All users (including GRETB staff, students, contractors, sub-contractors, agency staff and authorised third party commercial service providers) of GRETB's I.T resources;
- All use (both personal & GRETB business related) of GRETB's Information Technology (I.T.) resources;
- All connections to (locally or remotely) GRETB network Domains (LAN/WAN/Wi-Fi);
- All connections made to external networks through GRETB network.

3.0 Definitions

A list of terms used throughout this policy are defined in *Appendix A.*

4.0 Policy

4.1 Principles of Acceptable Use

The acceptable use of the Galway and Roscommon ETB's Information Technology (I.T.) resources is based on the following principles:

- All GRETB's I.T. resources and any information stored on them remain the property of GRETB.

- Users must ensure that they use Information Technology (I.T.) resources at all times in a manner which is lawful, ethical and efficient.

- Users must respect the rights and property of others, including privacy, confidentiality and intellectual property.

- Users must respect the integrity and security of GRETB's Information Technology (I.T.) resources.

4.2 Monitoring

- GRETB reserves the right to routinely monitor, log and record any and all use of its Information Technology (I.T.) resources for the purpose of:

    1) Helping to trace and resolve technical faults.
    2) Protecting and maintaining network and system security.
    3) Maintaining system performance and availability.
    4) Ensure the privacy and integrity of information stored on GRETB network.
    5) Investigating actual and suspected security incidents.
    6) Preventing, detecting and minimising inappropriate use.
    7) Protecting the rights and property of GRETB, its staff, learners and clients.
    8) Ensuring compliance with GRETB policies, current legislation and applicable regulations.

- Routine monitoring reports will be kept by GRETB for at least 30 days after which time they may be purged or deleted.

- While GRETB does not routinely monitor an individual user's use of its Information Technology (I.T.) resources it reserves the right to do so when a breach of its policies or illegal activity is suspected.

- The monitoring of an individual user will only be undertaken at the request of the individual's line manager (School/Centre Manager), the Chief Executive and the HR Department. The monitoring may include, but will not be limited to individual login sessions, details of information systems and records accessed, contents of hard disks, internet sites visited, time spent on the internet, telephone usage and the content of electronic communications.

- GRETB will at all times seek to act in a fair manner and respect the individual user's right for the privacy of their personal information under the Data Protection Acts 1988, 2003 and 2018. Information collected through monitoring will not be used for purposes other than those for which the monitoring was introduced, unless it is clearly in the users interest to do so or it reveals activity that GRETB could not be reasonably expected to ignore, for example a user found to be viewing, downloading or forwarding child pornography must be reported to Gardaí.

- Individual monitoring reports will only be accessible to the appropriate authorised GRETB personnel and will be deleted when they are no longer required.

- In the process of dealing with computer support calls GRETB IT staff may need to access a user's computer to resolve the support call. In such circumstances IT staff must respect the privacy of the individual user and not access information, documents or emails of a personal nature without the users permission or unless they need to in order to resolve the support call. In some cases the IT Department may use remote control software to connect and take control of a user's computer remotely. In such circumstances the IT staff will not use this software to connect to the user's computer without first attempting to contact the user of the computer first.

4.3 Personal Use

- GRETB's Information Technology (I.T.) resources are to be used primarily for GRETB business-related purposes. However at the discretion of their line manager occasional personal use may be permitted by a user provided it:

    1) Is not excessive;
    2) Does not take priority over their GRETB work responsibilities;
    3) It does not interfere with the performance and work of the user, other staff or GRETB;
    4) Does not incur unwarranted expense or liability for GRETB;
    5) Does not have a negative impact on GRETB in any way;
    6) Does not involve commercial activities, such as running any sort of private business, advertising or performing work for personal gain or profit;

7) Is lawful and complies with this policy and all other relevant GRETB policies

- GRETB has the final decision on deciding what constitutes excessive personal use.

- GRETB does not accept liability for any fraud or theft that results from a user's personal use of GRETB's Information Technology (I.T.) resources.

4.4 Confidentiality and Privacy

- Galway and Roscommon ETB is legally required under the *Irish Data Protection Acts 1988, 2003 and 2018* to ensure the security and confidentiality of all personal information it processes on behalf of its staff, clients and learners.

- In the course of a user's work for GRETB, he/she may have access to, or hear information concerning the sensitive or personal affairs of GRETB staff, learners or clients. Such information irrespective of the format (i.e. paper, electronic or otherwise) is strictly confidential and must always be safeguarded.

- Users must respect the privacy and confidentiality of information at all times. They must not access information or information systems unless they have a valid GRETB business related reason to do so or they have been granted permission by the information owner.

- Users must not remove any GRETB confidential or restricted information (irrespective of format) from GRETB location they are employed at without the authorisation of their line manager. Such authorisation must be issued in advance of the first instance and may apply thereafter if necessary. Where a user has been authorised to remove GRETB confidential or restricted information from a GRETB location they will be responsible for the safe transport and storage of the information.

- Confidential and restricted information must only be discussed or shared with others on a strict "need to know" basis.

- Confidential and restricted information must only be discussed or shared with other GRETB staff or staff of a GRETB funded agency who have a valid GRETB business related reason and are authorised to have access to the information.

- Confidential and restricted information must only be released and disclosed to the general public in accordance with the relevant legislation and agreed GRETB

procedures (for example, *Freedom of Information Acts 1997 and 2003, Data Protection Acts 1988, 2003 and 2018*).

- Confidential and restricted information must only be released and disclosed to other governmental agencies and departments in accordance with the relevant legislation (for example, *Freedom of Information Acts 1997 and 2003* / *Data Protection Acts 1988, 2003 and 2018 etc*.).

- Confidential and restricted information must only be released and disclosed to third party commercial service providers who have:

    1) A signed contract in place with GRETB for the provision of goods or services to GRETB, and;

    2) A valid legal and business reason for needing access to such information (for example: they require access to the information in order to provide the goods or services to GRETB), and;

    3) Signed a copy of the GRETB *Service Providers Confidentiality Agreement*

- Where it is necessary to release or disclose confidential or restricted information to third party commercial service providers only the minimum amount of information should be released as is absolutely necessary for a given function to be carried out by the commercial service provider on behalf of GRETB.

- Confidential or restricted information (irrespective of the format) must not be copied, renamed, deleted or modified without the authorisation of the information owner. This includes information on storage devices and information in transit.

- Users must not remove from their GRETB employment location any confidential or restricted information, (irrespective of the format - paper, electronic or otherwise) belonging to GRETB without the prior authorisation of their line manager.

- Personal information belonging to GRETB staff, learners or clients must not be used for presentations unless it has first been anonymised or psuedonymised otherwise the explicit consent of GRETB staff, learners or clients is required.

4.5 User Access Accounts & Passwords

- Where appropriate individual users will be granted access to GRETB's Information Technology (I.T.) resources which are necessary for them to perform their specific function for GRETB.

- Each authorised user will assigned an individual user access account name and password set which they can use to access a particular GRETB Information Technology (I.T.) resource. In some (limited) circumstances the use of generic / group access accounts is permitted.

- Each user is responsible for all activities performed on any GRETB I.T. device, information system or application while logged in under their individual access account and password.

- Users must ensure all passwords assigned to them are kept secure and private.

- Users who suspect their password is known by others must change their password immediately. Users can change their password using *Ctrl, Alt and Delete* or by contacting Helpdesk (helpdesk@gretb.ie).

- Users must ensure all default passwords which are supplied by a vendor for new GRETB I.T. devices and information systems are changed at installation time.

4.6 Software and Electronic Media

- Each user is responsible for making use of software and electronic media in accordance with the Irish *Copyright and Related Rights Act 2000* and software licensing agreements.

- Only software which has the correct and proper license may be installed and used within GRETB.

- Mobile and smart device application software (i.e. apps) must only be downloaded and installed on GRETB devices where there is a valid GRETB business reason and the software can add value for GRETB.

- All software and electronic media developed and purchased on behalf GRETB remains the property of GRETB and must not be used, copied, distributed or borrowed without the authorisation of GRETB.

- The IT Department on behalf of GRETB reserves the right to remove software at any time, for reasons including but not limited to (1) non-compliance with GRETB policies, (2) the software is not properly licensed, or (3) the software is found to have a negative impact on the performance of GRETB network, systems or equipment.

4.7 GRETB I.T. Devices & Equipment

- All GRETB I.T. devices and equipment must be purchased through the following agreed channels, GRETB contract agreements, IT framework agreements or directly through the IT Department.

- GRETB I.T. devices and equipment which has not been purchased through agreed channels must be approved by the IT Department before being allowed to connect to the GRETB network.

- All I.T. devices and equipment provided by GRETB remain the property of GRETB. Users must not remove or borrow GRETB I.T. devices or equipment without the authorisation of their line manager. The security of any GRETB I.T. devices and equipment borrowed is the responsibility of the borrower and the I.T. devices and equipment must be returned by the borrower before they leave the employment of GRETB or, at the request of the borrower's line manager or the IT Department.

- Users must not alter the hardware or software configuration of any GRETB I.T. device or equipment without the prior authorisation of the IT Department.

- Users must take due care when using GRETB I.T. devices and equipment and take reasonable steps to ensure that no damage is caused to the I.T. device or equipment. They must not use I.T. devices and equipment (either in a GRETB location, while traveling or at home) if they have reason to believe it is dangerous to themselves or others.

- Users must report all damaged, lost or stolen GRETB I.T. devices and equipment to their line manager and the IT Department.

- Old and obsolete GRETB I.T. devices and equipment must be recycled in accordance with the requirements of the European *Waste Electrical and Electronic Equipment (WEEE)* Directive and in accordance with the *GRETB Disposal of Assets Policy*.

- The IT Department on behalf of GRETB reserves the right to remove any I.T. devices and equipment from the network at anytime, for reasons including but not

limited to (1) non compliance with GRETB policies, (2) the I.T. device or equipment does not meet approved specification and standard, or (3) the I.T. device or equipment is deemed to be interfering with the operation of the network.

4.8 Laptops, Mobile Computer Devices & Smart Devices

- Users must ensure that GRETB laptops, mobile computer devices and smart devices provided to them are protected at all times. They must take all reasonable steps to ensure that no damage is caused to the device and the device is protected against loss or theft.

- GRETB mobile phones must only be issued to users who have signed a copy of *GRETB Mobile Phone Policy.*

- All GRETB smart devices must be registered with the IT Department so that they can be routed through GRETB network infrastructure and managed securely.

- GRETB laptops, mobile computer devices and smart devices must be password protected.

- Passwords used to access GRETB laptops, mobile computer devices and smart devices must not be written down on the device or stored with or near the device.

- Confidential and restricted information must only be stored on a GRETB laptop, mobile computer device or smart device with the authorisation of the user's line manager (School/Centre Manager). Such authorisation must be issued in advance of the information being stored on the device. Where authorisation has been granted only the minimum amount of confidential or restricted information must be stored on the device as is absolutely necessary for a given function to be carried out. Such information should be stored in GRETB's OneDrive for Business.

- When working in the office GRETB laptops, mobile computer devices and smart devices must be physically secured and positioned in such a way as to minimise the risk of theft. When they have to be left unattended for any period of time and at the end of the each working day the devices should be secured to a desk or some other stationary object using an appropriate locking mechanism (i.e. Laptop / iPad cable lock) or locked in a drawer or filing cabinet.

- GRETB laptops, mobile computer devices and smart devices must not be left unattended when working off-site.

- When traveling by car, GRETB laptops, mobile computer devices and smart devices should be stored securely out of sight when not in use. Avoid leaving the devices unattended in the boot of a car overnight.

- The use of GRETB devices within a car must at all times be made in accordance with the *Road Traffic Act 2006.*

- When traveling by taxi, train or plane GRETB laptops, mobile computer devices and smart device's should be kept close to hand at all times. Avoid placing the devices in locations where they could easily be forgotten or left behind (i.e. in overhead racks or boots of taxis).

- When using a GRETB laptop, mobile computer devices or smart device in a public place users need to take precautions to ensure the information on the device screen cannot be viewed by others.

- Users must ensure that all GRETB laptops, mobile computer devices and smart devices provided to them are not accessed (including internet access) by persons who are not GRETB Staff (i.e. friends, family members and others etc.).

4.9 GRETB Network

- Access rights and privileges to GRETB network domains and network resources will be allocated based on the specific requirement of a users GRETB role / function, rather than on their status.

- Access to GRETB network domains will generally be controlled by the use of individual user access account's, however in certain (limited) circumstances the use of generic or group accounts maybe permitted.

- Users must not:

    1) Disconnect any GRETB I.T. devices, equipment or storage devices from a GRETB network domain without the prior authorisation of the IT Department.

    2) Connect any GRETB I.T. devices and equipment, laptop or smart device to an external network without the prior authorisation of the IT Department.

3) Connect any I.T. devices and equipment, laptop, smart device, mobile phone device or storage device which is their personal property and is not owned or leased by GRETB to a GRETB network domain without the prior authorisation of the IT Department

- All activity on GRETB network domains is routinely monitored, logged and recorded for the purposes of helping to trace and resolve technical faults and investigating actual and suspected security breaches(See section 4.2).

4.10 Email

- Email is provided for administrative and teaching and learning functions. Please refer to Section 4.3.

4.11 Internet

- Internet is provided for administrative and teaching and learning functions. Please refer to Section 4.3.

4.12 Telephone System

- Access to GRETB telephone system is primarily intended for GRETB work related purposes. The making and taking of personal calls is allowable provided users keep these to a minimum.

- Users must respect the privacy of others at all times and not attempt to access calls where the user is not the intended recipient or log into voice mail accounts that the user is not expressly authorised to access.

- The use of GRETB mobile phone devices is governed by the requirements of GRETB *Mobile Phone Policy.*

4.13 Information Backup

- Information on GRETB networked servers will be automatically backed up on a daily basis. School/Centre Managers should seek confirmation from the IT Department.

- Users who do not have access to a GRETB network server must ensure that they regularly backup all their important information onto GRETB's OneDrive for

Business. Each user is responsible for ensuring their backup information is kept safe and secure.

- Information backups especially those containing confidential and restricted information must be stored securely e.g. by IT or on your GRETB OneDrive for Business.

- Information backups should be regularly tested to ensure that a recovery can take place following an incident or hardware/software failure.

4.14 Virus & Malicious Software Protection

- The IT Department will ensure virus scanning software is available on every GRETB desktop and laptop computer device that is connected to GRETB network and undertake the regular updating of such virus scanning software. Due to their nature standalone desktop computers and laptops which are not regularly connected to GRETB network are unlikely to have fully up to date virus protection. Please contact IT if you require confirmation.

- The IT Department is not responsible for supplying or updating virus scanning software on computer devices which are not owned or leased by GRETB.

- Users who receive a virus warning message should contact the IT Department to determine the authenticity of the warning. Under no circumstances should they forward it on to other users.

4.15 Information Storage

4.15.1 GRETB On-Site Server Storage

- For security and legal reason GRETB's preferred position is that:

    1) All GRETB confidential or restricted information is stored on a GRETB network server or on the GRETB SharePoint or OneDrive for Business.

- GRETB network servers are reserved for the hosting/storage of GRETB business-related systems and information only. Users must store all non-GRETB personal information (i.e. information which is of a personal nature and belongs to the user and not GRETB) on their local GRETB computer device.

4.15.2 Third Party Storage Facilities

- In special circumstances such as when business, technical (i.e. specialised system support etc.), security (i.e. disaster recovery backup etc.) or legal (i.e. archiving,) requirements necessitate GRETB confidential or restricted information and/or information systems maybe physically stored off-site at a third party storage facility or hosted off-site on third party servers and equipment.

- Where GRETB confidential information, restricted information or information systems are physically stored off-site at a third party storage facility or hosted offsite on third party servers and equipment GRETB's preferred position is that third party storage facility, servers and equipment are (1) located within the Republic of Ireland or failing that, (2) they are located within a country which is a member of the European Economic Area (EEA).

- In exceptional circumstances GRETB may consider requests to store / host GRETB confidential information, restricted information or information systems on third party servers and equipment which are located in a country outside the European Economic Area (EEA). Each request will be evaluated on a case by case basis and will take into account the sensitivity of the information involved, data protection law and any other legal issues, available alternatives, support issues, logistics and the security controls in place.

- The storage / hosting of GRETB confidential and restricted information and information systems off-site at third party storage facilities or on third party servers and equipment must be approved by the relevant information owner.

- GRETB confidential information, restricted information and information systems may only be stored /hosted off-site at third party storage facilities or on third party servers and equipment, when:

    1) GRETB has satisfied its self that the third party storing / hosting GRETB information and information systems has the appropriate human, organisational and technological controls in place to protect GRETB information and information systems against unauthorised access and disclosure, accidental loss, destruction, deterioration, damage and alteration, and;

    2) A signed legal contract exists between GRETB and the third party governing the processing or storage of GRETB information and/or information systems, and;

    3) The third party has signed a copy of GRETB *Service Provider*

Confidentiality Agreement

4.15.3 Storage on Personal I.T. Devices & Equipment

- Users are strictly prohibited from hosting/storing GRETB confidential information, restricted information or information systems on any computer device, mobile computer device, smart device, mobile phone device, removable storage device, photographic, video or audio recording device or any other equipment which is their personal property and is not owned or leased by GRETB.

4.16 Physical Security

- GRETB I.T. devices and equipment must be physically secured and positioned in such a way as to minimise the risk of unauthorised individuals accessing the device or viewing information displayed on the device screen.

4.16.1 GRETB Network Servers & data communications Equipment

- Critical GRETB network and data communication equipment (for example, switches, routers, hubs, patch panels etc) should be placed in communications racks or cabinets and located within accessed controlled areas (i.e., a server / comms room or a locked room) which are only accessible to authorised GRETB staff.

- Power and communications cabling carrying data or supporting key information systems should be protected from interception and damage.

- Local server / comms rooms or other areas housing GRETB network servers and/or network and data communication equipment situated on the ground floor should have all windows kept shut or where possible.

- Hazardous and combustible materials must not be stored within or near GRETB local server / comms rooms or other areas housing GRETB network servers and/or network and data communication equipment.

4.16.2 GRETB Computers & Peripheral Devices

- Users should operate a clear screen policy and log off or 'lock' their GRETB computer (using *Ctrl+Alt+Delete* keys) when they have to leave it unattended for any period of time. Computers automatically power off each night at 22:15.

- Where practical users should operate a clear desk policy and clear their desks of all confidential and restricted information (irrespective of the format) at the end of each working day or when leaving their workplace for a major part of the day,

- Storage devices, GRETB approved USB memory sticks, mobile phone devices, laptops, smart devices and photographic, video and audio recording devices should be stored away in a secure location when not in use.

- Where possible, fax machines, printers, scanners and photocopiers which are used to regularly fax, print, scan or copy confidential or restricted information should be located within areas which are not accessible by the general public.

- Confidential and restricted information, when faxed, printed, scanned or copied should where practical be collected from the fax machine, printer, scanner or photocopier immediately.

4.17 Information Transfer

- Transfer(s) of confidential or restricted information to third parties must be authorised by a GRETB line manager (School/Centre Manager). Such authorisation must be issued in advance of the first instance and may apply thereafter if necessary.

- Where it is necessary to transfer confidential or restricted information to third parties, only the minimum amount of information should be transferred as is necessary for a given task to be carried out.

- Where possible all transfer(s) of confidential and restricted information should take place electronically via secure channels (i.e. Secure FTP, TLS, VPN etc) or encrypted email or the GRETB OneDrive for Business.

- In circumstances where electronic transfer is not possible, users should contact IT.

- All transfer(s) of personal information to third parties must be legally justified and made in accordance with the *Data Protection Acts 1988, 2003 and 2018.*

- When transferring personal information to a third party located outside the Republic of Ireland there are a number of additional requirements and legal obligations that need to be considered. If any user has a need to transfer personal information outside the Republic of Ireland they must contact the Data Protection Office at data.protection@gretb.ie.

4.18 Information Disposal

- Confidential and restricted information must be securely deleted when it is no longer required.

- All traces of confidential and restricted information must be purged from old GRETB computers, smart devices, mobile computer devices, mobile phone devices and storage devices before they are reused and must be in accordance with the *GRETB Disposal of Assets Policy*.

- The simple deletion or formatting of information stored on a device is not sufficient to remove all traces of the information. The information must be purged by either (1) using special sanitation software to overwrite the information a number of times, or (2) the hard disk must be degaussed (i.e. information is permanently purged using a powerful magnet) or (3) the physical destruction of the media (i.e. hard disk, magnetic tape, video & audio tapes, CD/DVD's, floppy disks etc) the information is stored on.

- Photocopiers and scanners which are fitted with hard disks must be purged of all confidential and personal data before they are disposed of or returned to the vendor.

- Computers and other I.T. equipment which are leased from third parties must be purged of all confidential and personal data before being returned to the third party leasing company.

- Where the disposal of old GRETB computer equipment and removable storage devices is outsourced to a commercial service provider the commercial service provider must:

    1) Ensure the operation of purging the computer equipment of all confidential and restricted information and the destruction of the media (i.e. hard disk, magnetic tape, video & audio tapes, CD/DVD's, floppy disks etc.) is carried out on-site at a GRETB location before the equipment is taken off-site to a licensed WEEE recycling facility within Ireland.

2) Provide GRETB with a certificate of disposal / destruction for all the equipment that was disposed of / destroyed by them.

3) Signed a copy of GRETB *Service Providers Confidentiality Agreement*

4.19 Working from Home (Home Working)

- Users who are authorised by GRETB to work from home (home workers) must take all reasonable measures to ensure all GRETB computer devices provided to them are kept secure and are protected against unauthorised access, damage, loss, theft and computer viruses.

- Users who work from home must ensure:

1) All work carried out by them on behalf of GRETB while working at home is processed and stored on a GRETB computer device and not any other device which is their personal property or the personal property of another household member;

2) All GRETB computer devices used by them to work from home are password protected.

3) All GRETB computer devices used by them to work from home have GRETB approved encryption software installed;

4) All GRETB computer devices used by them to work from home have GRETB approved anti-virus software installed and this is kept up to date;

5) All confidential and restricted information which is accessed by them or stored on a GRETB computer device provided to them is kept secure and confidential at all times;

6) All GRETB computer devices and information provided to them are not accessed (including internet access) by members of their family, other household members or visitors;

7) All GRETB computer devices and information (irrespective of the format) are securely locked away when not in use;

8) All old printouts, faxes and other paper based records that contain confidential or restricted information are shredded or disposed of securely and are not disposed along with their ordinary household rubbish;

- All computer devices provided by GRETB remain the property of GRETB and must be returned to GRETB by the home worker before they leave the employment of GRETB or at the request of their GRETB line manager or the IT Department.

4.20 Periods of Absence

- During planned periods of absence such as career breaks, holidays, on training courses or working off-site for an extended period of time, users should ensure wherever possible that their line manager or work colleagues have access to important GRETB business related documents and email messages stored on their computer so that there is no disruption to service delivery.

- During unplanned periods of absence such as ill health, or where a user has forgotten to provide access to their line manager or work colleagues, the user's line manager may be permitted to access their computer to retrieve GRETB business related documents or emails messages so as to minimise any disruption to service delivery. In such circumstances line managers must respect the privacy of the user and not access documents or emails of a personal nature unless there are compelling conditions that warrant doing so.

4.21 Users leaving GRETB & User Transfers

- Users must return all GRETB mobile phone devices and accessories (e.g. mobile battery charger etc), computer equipment (e.g. laptop, smart devices, storage devices, USB memory sticks etc), information (i.e. documents, files, important email messages etc) and other important items (e.g. swipe cards, keys, parking permit and I.D. badge etc) to their GRETB line manager before they leave the employment of GRETB.

- Line managers must contact the IT Department to ensure that the information system and network access accounts belonging to users leaving the employment of GRETB are revoked immediately once they leave the organisation.

- Users leaving the employment of GRETB should also ensure they remove or delete all non-GRETB personal information & email messages (i.e. information / email messages which are of a personal nature and belong to the user and not GRETB) from their GRETB mobile phone device and computer equipment before

they leave as it may not be possible to get a copy of this data once they have left GRETB.

- At the discretion of the IT Department users who are retiring or resigning from GRETB may by agreement purchase their GRETB mobile phone device and computer equipment from GRETB for their current value. The current value of the mobile phone device and computer equipment will be set by the Finance Department.

- Users who are transferring internally within GRETB must ensure they return all GRETB mobile phone devices and accessories, laptops, and swipe cards etc to their current GRETB line manager before they transfer. They must also ensure that their current line manager or work colleagues have access to important GRETB business related documents and email messages so that there is no disruption to service delivery after they transfer.

- Line managers must contact the IT Department to ensure that access account privileges that are no longer required by a user as a result of them transferring internally within GRETB are removed.

4.22 Information Security Breach

- Information security breaches include but are not limited to the following (1) the loss or theft of a computer device containing confidential or restricted information, (2) the loss or theft of a photographic, video or audio recording device containing confidential or restricted information, (3) the loss or theft of a USB memory stick or some other form of removable storage device containing confidential or restricted information, (4) the transmitting of confidential or restricted information an incorrect person, (5) incidents where confidential or restricted information was mistakenly or otherwise disclosed to unauthorised persons.

- Users must report all actual or suspected information security breaches immediately to their line manager, the IT Department and/or the Data Protection Office.

4.23 Unacceptable Use

GRETB's Information Technology (I.T.) resources must not be used:

1) For excessive personal use;
2) For commercial activities, such as running any sort of private business, advertising or performing work for personal gain or profit;
3) For political activities, such as promoting a political party / movement, or a candidate for political office, or campaigning for or against government decisions;
4) To knowingly misrepresent GRETB;
5) To transmit confidential or restricted information outside GRETB unless the information has been encrypted and transmission has been authorised by their GRETB line manager (School/Centre Manager);
6) To store or transfer confidential or restricted information(encrypted or otherwise) onto an **unapproved** USB memory stick;
7) To enter into contractual agreements inappropriately (i.e. without authorisation or where another form of agreement is required);
8) To create, view, download, host or transmit material (other than users who are authorised by GRETB to access such material for research etc.) of a pornographic or sexual nature or which may generally be considered offensive or obscene and could cause offence to others on the grounds of race, creed, gender, sexual orientation, disability, age or political beliefs. material is defined as information (irrespective of format), images, video clips, audio recordings etc;
9) To retrieve, create, host or transmit material which is designed to cause annoyance, inconvenience or needless anxiety to others;
10) To retrieve, create, host or transmit material which is defamatory;
11) For any activity that would infringe intellectual property rights (e.g. unlicensed installation, distribution or copying of copyrighted material);
12) For any activity that would compromise the privacy of others;
13) For any activity that would intentionally cause disruption to the computer systems, telephone systems or networks belonging to GRETB or others;
14) For any activity that would deliberately cause the corruption or destruction of data belonging to GRETB or others;
15) For any activity that would intentionally waste GRETB's resources (e.g. staff time and Information Technology (I.T.) resources);
16) For any activity that would intentionally compromise the security of GRETB's Information Technology (I.T.) resources, including the confidentiality and

integrity of information and availability of IT resources (e.g. by deliberately or carelessly causing computer virus and malicious software infection);

17) For the installation and use of software or hardware tools which could be used to probe or break GRETB I.T. security controls;
18) For the installation and use of software or hardware tools which could be used for the unauthorised monitoring of electronic communications within GRETB or elsewhere;
19) To gain access to information systems or information belonging to GRETB or others which you are not authorised to use;
20) For creating or transmitting "junk" or "spam" emails. This includes but is not limited to unsolicited commercial emails, jokes, chain-letters or advertisements;
21) For any activity that would constitute a criminal offence, give rise to a civil liability or otherwise violate any law.

- The above list should not be seen as exhaustive, as other examples of unacceptable use of GRETB's I.T. resources may exist.
- GRETB has the final decision on deciding what constitutes excessive personal use.
- GRETB will refer any use of its I.T. resources for illegal activities to the Gardai.

5.0 Roles & Responsibilities

5.1 IT Department

The IT Department is responsible for:

- The provision of reliable computer systems which deploy appropriate technical safeguards against threats to their availability, operation, stability, and performance;
- The management and security of GRETB network(LAN/WAN);
- The provision of facilities for information backups on GRETB network file servers and other centralised information stores but excluding backups of the hard disks on individual computers;
- The provision and management of anti virus/spyware software throughout GRETB.
- The provision, deployment and management of encryption facilities throughout GRETB.
- The provision of additional security measures to enable use of computer systems outside the normal working environment when this is appropriate and necessary;

- The procurement of all IT networking equipment, software and services;
- The installation of all software;
- The installation of all IT equipment, including connection to GRETB network;
- The provision of training, advice and guidance to computer systems users.

5.2 School/Centre Managers

Line managers are responsible for:

- The implementation of this policy and all other relevant GRETB policies within the business areas for which they are responsible;

- Ensuring that all GRETB staff, students, contractors, sub-contractors and agency staff who report to them are made aware of and have access to this policy and all other relevant GRETB policies;

- Ensuring staff, students, contractors, sub-contractors and agency staff who report to them return all GRETB computer devices (e.g. laptop, smart devices, printer, mobile phone devices, removable storage devices etc), information, important email messages and other important items (e.g. swipe cards, keys and I.D. badge etc) before they leave the employment of GRETB or transfer to another GRETB directorate or service area;

- Reporting all actual or suspected information security breaches immediately to the IT Department and/or the Data Protection Office;

- Consulting with the HR Department in relation to the appropriate procedures to follow when a breach of this policy has occurred.

5.3 Users

Each user of GRETB's I.T. resources is responsible for:

- Complying with the terms of this policy and all other relevant GRETB policies, procedures, regulations and applicable legislation;

- Respecting and protecting the privacy and confidentiality of the information systems and network they access, and the information processed by those systems or networks;

- Ensuring they only use user access accounts and passwords which have been assigned to them;

- Ensuring all passwords assigned to them are kept confidential at all times and not shared with others;

- Complying with instructions issued by designated information owners, system administrators, network administrators and/or the IT Department on behalf of GRETB;

- Reporting all lost, stolen or damaged I.T. devices to their line manager and the IT Department;

- Reporting all actual or suspected information security breaches immediately to their line manager, the IT Department and/or the Data Protection Office;

- Reporting all misuse and breaches of this policy to their line manager;

- Ensuring they return to their line manager, all GRETB computer devices (e.g. laptop, smart devices, printer, mobile phone devices, removable storage devices etc), information, important email messages and other important items (e.g. swipe cards, keys and I.D. badge etc) before they leave the employment of GRETB or transfer to another GRETB directorate or service area.

- Ensuring they remove or delete all non-GRETB personal information and email messages (i.e. information which is of a personal nature and belongs to the user and not GRETB) from their GRETB computer before they leave the employment of GRETB, as it may not be possible to get a copy of this data from GRETB once the user has left GRETB.

5.4 Network Administrators

Each GRETB network administrator is responsible for:

- Complying with the terms of this policy and all other relevant GRETB policies, procedures, regulations and applicable legislation.

5.5 System Administrators

Each GRETB system administrator is responsible for:

- Complying with the terms of this policy and all other relevant GRETB policies, procedures, regulations and applicable legislation;

- Complying with instructions issued by the IT Department on behalf of GRETB.

6.0 Enforcement

- GRETB reserves the right to take such action as it deems appropriate against individuals who breach the conditions of this policy. GRETB staff, students, contractors, sub-contractors or agency staff who breach this policy maybe subject to disciplinary action, including suspension and dismissal as provided for in GRETB disciplinary procedure.

- Breaches of this policy by a third party commercial service providers, may lead to the withdrawal of GRETB information technology resources to that third party commercial service provider and/or the cancellation of any contract(s) between GRETB and the third party commercial service provider.
- GRETB will refer any use of its I.T. resources for illegal activities to the Gardai.

7.0 Review & Update

This policy will be reviewed and updated annually or more frequently if necessary to ensure any changes to GRETB's organisation structure and business practices are properly reflected in the policy.

The most up to date version of this policy will be published on GRETB's SharePoint.

Appendix A

Anonymised / Anonymisation: The process of rendering data into an irrevocable form which does not identify any individual and can no longer be linked to an individual.

Authorisation / Authorised: Official GRETB approval and permission to perform a particular task.

Backup: The process of taking copies of important files and other information stored on a computer to ensure they will be preserved in case of equipment failure, loss or theft etc.

Breach of Information Security: The situation where GRETB confidential or restricted information has been put at risk of unauthorised disclosure as a result of the loss or theft of the information or, through the accidental or deliberate release of the information.

Confidential information: Information which is protected by Irish and/or E.U. legislation or regulations, GRETB policies or legal contracts. The unauthorised or accidental disclosure of this information could adversely impact GRETB, its Learners, its staff and its business partners. Some examples of confidential information include:

- Learner / client / staff personal data (Except that which is restricted)
- Learner /client / staff medical records (Except that which is restricted)
- Unpublished medical research
- Staff personal records
- Financial data / budgetary Reports
- Service plans / service performance monitoring reports
- Draft reports
- Audit reports
- Purchasing information
- Vendor contracts / Commercially sensitive data
- Data covered by Non-Disclosure Agreements
- Passwords / cryptographic private keys
- Data collected as part of criminal/HR investigations
- Incident Reports

Defamatory: False statement or series of statements which affect the reputation of a person or an organisation.

Electronic Media: Any Information that has been created and is stored in an electronic format, including but not limited to software, electronic documents, photographs, video and audio recordings.

Encryption / Encrypt: The process of converting (encoding) information from a readable form (plain text) that can be read by everyone into an unreadable form (cipher text) that can only be read by the information owner and other authorised persons.

Encryption Key: A piece of data (parameter usually a password) used to encrypt/decrypt information.

Generic / Group Access Account: An access account that is intended for use by a number of different people and not an individual user and as such is not derived from a single user's name.

Home Working: The situation where GRETB staff carry out their contractual obligations (either on an occasional or regular basis) on behalf of GRETB while working from their home instead of a GRETB location.

Home Worker(s): GRETB Staff are authorised to work from their home (on an occasional or regular basis) instead of a GRETB location.

GRETB Network: The data communication system that interconnects different GRETB Local Area Networks (LAN), Wide Area Networks (WAN) and Wi-Fi Wireless Networks.

GRETB Server: A computer on GRETB network used to provide network services and/or manage network resources.

Information: Any data in an electronic format that is capable of being processed or has already been processed.

Information Owner: The individual responsible for the management of a GRETB directorate or service (GRETB RDO or National Director **(**or equivalent)).

Information System: A computerised system or software application used to access, record, store, gather and process information.

Information Technology (I.T.) resources: Includes all I.T. devices and equipment, computer facilities, networks, data & telecommunications systems, equipment and infrastructure, internet/intranet and email facilities, software, information systems and applications, account usernames and passwords, and information and data that are owned or leased by GRETB.

Intellectual Property: Any material which is protected by copyright law and gives the copyright holder the exclusive right to control reproduction or use of the material. For example - books, movies, sound recordings, music, photographs software etc.

Line manager: The individual a user reports directly to.

Mobile Computer Device: Any handheld computer device including but not limited to laptops, tablets, notebooks, PDA's etc.

Mobile Phone Device: Any wireless telephone device not physically connected to a landline telephone system. Including but not limited to mobile phones, smart phone devices (for example, Apple iPhones, Windows Mobile enabled devices, Google Android enabled devices, Nokia Symbian enabled devices, Blackberry RIM enabled devices etc). This does not include cordless telephones which are an extension of a telephone physically connected to a landline telephone system.

Network Administrators: These are the individuals responsible for the day to day management of a GRETB network domain. Also includes GRETB personnel who have been authorised to create and manage user accounts and passwords on a GRETB network domain

Network Domain: A set of connected network resources (Servers, Computers, Printers, Applications) that can be accessed and administered as group with a common set of rules

Personal Information: Information relating to a living individual (i.e. GRETB Staff, or Learner or client) who is or can be identified either from the information or from the information in conjunction with other information. For example: - an individuals name, address, email address, photograph, date of birth, fingerprint, racial or ethnic origin, physical or mental health, sexual life, religious or philosophical beliefs, trade union membership, political views, criminal convictions etc.

Personal Use: The use of GRETB's Information Technology (IT) resources for any activity(s) which is not GRETB work-related.

Pornography / Pornographic: The description or depiction of sexual acts or naked people that are designed to be sexually exciting.

Privacy: The right of individual or group to exclude themselves or information about themselves from being made public.

Process / Processed / Processing: Performing any manual or automated operation or set of operations on information including:

- Obtaining, recording or keeping the information;
- Collecting, organising, storing, altering or adapting the information;
- Retrieving, consulting or using the information;

- Disclosing the information or data by transmitting, disseminating or otherwise making it available;
- Aligning, combining, blocking, erasing or destroying the information.

Psuedonymised / Pseudonymisation: Is a process which involves the replacement of all personal identifiers (i.e. an individual's name address etc) contained within information with artificial identifiers (for example replacing an individual's name and address with their initials or some other code etc). The purpose of pseudonymisation is to make it difficult for any unauthorised third parties to identify any individual(s) from the information, but to allow the organisation who psuedonymisaed the information in the first place to trace back the information to its origins.

Removable Storage Device: Any optical or magnetic storage device or media, including but not limited to floppy disks, CD, DVD, magnetic tapes, ZIP disk, USB flash drive (i.e. memory stick/pen/keys), external/portable hard drives.

Restricted Information: Highly sensitive confidential information**.** The unauthorised or accidental disclosure of this information would seriously and adversely impact GRETB, its learners, its staff and its business partners. Some examples of restricted information include:

- Learner / client / staff sensitive restricted information
- Unpublished financial reports
- Strategic corporate plans
- Sensitive research

Smart Device: A handheld mobile computer device which is capable of wireless connection (via WiFi, 3G, 4G etc), voice and video communication and, internet browsing. (for example: Apple IOS enabled devices (i.e. iPhone & iPad), Google Android enabled devices (i.e. Samsung Galaxy tablet), Windows Mobile enabled devices and, Blackberry RIM enabled devices etc)

Social Media: The name given to various online technology tools that enable people to communicate easily via the internet to share information and resources. It includes the following types of web sites:

1) **Internet Chat Rooms:** Websites that allow interactive messaging, where users can exchange views and opinions in real time on a variety of subject matters.

2) **Internet Discussion Forums/Message Boards:** Websites that allow users to participate in on-line discussions on a particular subject matter.

3) **Internet Social Networking Websites:** Websites that allow users to build on-line profiles, share information, pictures, blog entries and music clips etc. Including but not limited to Bebo, Facebook, Twitter, Myspace, Friendster, Whispurr, LinkedIn and Viadeo.

4) **Internet Video Hosting/ Sharing Websites:** Websites that allows users to upload video clips, which can then be viewed by other users. Including but not limited to Youtube, Yahoo Video, Google Video and MyVideo.

5) **Blogging Websites:** Websites that allow a user to write an on-line diary (known as a blog) sharing their thoughts and opinions on various subjects

Software: A computer program or procedure that enables a computer to perform a particular task.

System Administrators: The individual(s) charged by the designated system owner with the day to day management of GRETB information systems. Also includes GRETB personnel and third parties who have been authorised to create and manage user accounts and passwords on these applications and systems.

Third Party Commercial Service Provider: Any individual or commercial company that have been contracted by GRETB to provide goods and/or services (for example, project / contract management, consultancy, information system development and/or support, supply and/or support of computer software / hardware, equipment maintenance, data management services, Learner / client care and management services etc.) to GRETB.

Third Party Servers and Equipment: Any servers or computer equipment used to store or host GRETB information and/or information systems which are not owned by GRETB.

Third Party Storage Facilities: Any location or facility used to store GRETB information, information systems and/or computer equipment which is not owned or managed by GRETB.

Users: Any authorised individual who uses GRETB's I.T. resources.