Computer use, access and security

Seirbhís Phríosúin na hÉireann
IRISH PRISON SERVICE

Policy Document

Policy Index No.	Policy Sponsor	Page/s	Approved by	Date
PIN006	Information and Communications Technology Section & Staff and Corporate Services Directorate	32	Directors of Estates and ICT and Staff and Corporate Services	10/12/14

Related policies/standards	Date
026 IPS Social Media Policy	10/12/14
The Data Protection Acts 1998 and 2003,	
The Official Secrets Act 1963.	
See Section 5	

Legacy reference of policy	Date for review of policy	Date of issue/amendment
-	10/12/2015	10/12/2014

IPS Policy for Computer Use, Access and Security

Table of Contents

1. Aim of this policy

1.1 Information and Communications Technology (ICT) is critical to the successful operation of the Irish Prison Service (IPS). It has automated manual processes and has facilitated the development and delivery of new services to the public, staff and prisoners. This policy aims to ensure that ICT within the IPS is used responsibly and through its use, the business of the IPS is not put at risk.

2. Purpose of this policy

2.1 Our reputation depends on our capacity to deliver a quality service to the Minister, the Government, other Government Departments, Public Bodies, the Secretary General, the MAC, the Director General, the Directors and Governors, and of course the public. All steps must be taken to prevent damage to that reputation. Therefore the purpose of this policy is as follows.

2.1.1 To define the correct and proper use of the IPS ICT resources and infrastructure as they affect users. ICT resources includes, but is not limited to personal computers (PCs), servers, storage, network, telephone, mobile computer device (laptop, smart phone, tablet, PDA), USB memory keys, fax, instant messaging, mobile phone, video conferencing, email, internet, intranet (IRIS) & remote access.

2.1.2 To state the standards of behaviour, interaction with and use of the ICT facilities that is expected from users in order to protect the confidentiality, integrity and availability of information and to protect the reputation of the IPS and its staff.

2.1.3 To explain to users the main reasons why the measures outlined are necessary.

3. Scope of this policy

3.1 This policy represents the IPS national position. The Policy applies to:

3.1.1 All ICT resources provided by the IPS.

3.1.2 All users, holders and uses of IPS ICT resources.

3.1.3 All connections to the IPS network (LAN/WAN/Wireless/PSTN).

3.1.4 All *connections made to external networks through the IPS network.*

3.2 It is vital that you read this policy carefully and apply it in the use of IPS ICT resources. If there is anything that you do not understand, it is your responsibility to ask your ICT Coordinator, line manager, Staff and Corporate Services (SCS) Directorate or IPS ICT Section to explain it to you.

3.3 All users of ICT equipment must comply with all current Irish legislation. All users will ensure that their usage of any of the ICT resources provided by the IPS will not contravene any of the legislative acts and regulatory requirements, including the more common ones listed in Appendix B. *Information for the purposes of this policy includes data in an electronic format that is capable of being processed or has already been processed.*

3.4 If you have any concerns signing up to accept this policy, please email SCS at staffqueries@irishprisons.ie or phone 043 3335377.

3.5 If you have any queries in relation to the technical requirements in the policy, please email the IPS ICT Helpdesk at itsupport@irishprisons.ie or phone 043 3335333.

3.6 All exceptions to this policy must be authorised by the Director of Estates/ICS and/or Head of ICT or Director of Staff and Corporate Services. Exception requests must be submitted in writing using the Computer Use, Access and Security Policy Exception Request Form found on the ICT section of IRIS and a completed copy sent by e-mail to itsupport@irishprisons.ie or by fax to 043 3335252.

4. Roles and Responsibilities

4.1 IPS ICT Section

4.1.1 The IPS ICT Section is responsible for:

a) The procurement of all ICT equipment and services.

b) The installation and provision of all ICT equipment, including connection to the IPS and the education network.

c) The management and security of the IPS network (LAN/WAN/Wireless/PSTN).

d) The provision of facilities for information backups on IPS file servers and other centralized information stores but excluding backups of the hard disks on individual computers.

e) The provision and management of security software and systems throughout the IPS e.g. anti virus and firewalls.

f) The provision of additional security measures to enable use of computer systems outside the normal working environment when this is appropriate and necessary.

g) The provision, deployment and management of encryption facilities throughout the IPS.

h) The installation of all licensed software.

i) The provision of training, advice and guidance to ICT users.

j) The publication of all ICT policies.

4.1.2 Where a potential breach of this policy is notified to the SCS or to ICT Section, the Head of ICT or a senior deputy will investigate the potential breach. The Head of ICT or a senior deputy will determine if there is an actual breach of the policy. If an actual breach has occurred the Head of ICT or a senior deputy will investigate the breach from a technical perspective and then notify the SCS Directorate of their findings. It will then be a decision for the SCS Directorate to determine what further action to carry out.

4.2 Information Owners

4.2.1 Information owners are responsible for:

a) The implementation of this policy and all other relevant policies within the IPS Directorates they manage and Prison Institutions.

b) In conjunction with the ICT Section , the ownership, management, control and security of the information processed by their Directorate or service on behalf of the IPS and Prison Institutions.

c) In conjunction with the ICT Section, the ownership, management, control and security of IPS information systems used by their Directorate or Service to process information on behalf of the IPS

d) In conjunction with the ICT Section, maintaining a list of IPS information systems and applications that are managed and controlled by their Directorate or Service.

e) Making sure adequate procedures are implemented within their Directorate or Service so as to ensure all IPS employees, third parties and others that report to them are made aware of, and are instructed to comply with this policy and all other relevant policies.

4.3 Governors/Directors & line managers

4.3.1 Governors/Directors and line managers are responsible for:

a) The implementation of this policy and all other relevant policies within the business areas for which they are responsible.

b) Ensuring that all IPS employees who report to them are made aware of and are instructed to comply with this policy and all other relevant IPS policies.

c) Ensuring IPS employees who report to them return all IPS computer devices (e.g. laptop, mobile, removable storage devices, etc), information and other important items (e.g. swipe cards, keys and I.D. badge, etc) before they leave the employment of the IPS or transfer to another IPS directorate or service area.

d) Consulting with the SCS Directorate in relation to the appropriate procedures to follow when a breach of this policy has occurred.

4.4 IPS Staff/Officers/Contractors & Third Parties

4.4.1 Each user of IPS ICT resources is responsible for:

a) Complying with the terms of this policy and all other relevant IPS policies, procedures, regulations and applicable legislation.

b) Respecting and protecting the privacy and confidentiality of the information systems and networks they access, and the information processed by those systems or networks.

c) Using ICT resources in a responsible manner respecting the dignity of all colleagues, prisoners ex-prisoners IPS employees or any other persons working in our prisons in compliance with the IPS Anti-Harassment Sexual Harassment and Bullying Policy.

d) Ensuring they only use user access accounts and passwords which have been assigned to them.

e) Ensuring all passwords assigned to them are kept confidential at all times and not shared with others.

f) Changing their passwords at least every 90 days or when instructed to do so by designated system administrators, network administrators or the ICT Section.

g) Complying with instructions issued by designated information owners, system administrators, network administrators and/or the IPS ICT Section on behalf of the IPS.

h) Reporting all lost, stolen or damaged ICT devices to their line manager/Governor and the ICT Section.

i) Reporting all actual or suspected breaches of information security immediately to their line manager/Governor or the ICT Section

j) Reporting all misuse and breaches of any element of this policy to their line manager.

k) Staff should not attempt to repair and/or disassemble any ICT equipment or remove any part(s). All damaged/decommissioned ICT equipment must be immediately reported to ICT and if instructed, returned to ICT for repair or safe/secure disposal

l) Ensuring they return to the ICT Section, all IPS computer devices (e.g. laptop, mobile, removable storage devices, etc), information and other important items (e.g. swipe cards, keys and I.D. badge, etc) before they leave the employment of the IPS or transfer to another IPS Directorate or Service area.

4.4.2 While the IPS ICT Section and SCS Directorates are responsible for writing and publishing IPS ICT policies and best practices guidelines, their successful implementation is dependent on every user complying and adhering to them. If anyone has any recommendations on how these policies could be improved, send your feed back to the IPS ICT Helpdesk at itsupport@irishprisons.ie or phone 043 3335333.

4.5 Acceptable Use

The acceptable use of the ICT resources is based on the following principles:

4.5.1 The IPS ICT resources are to be used primarily for IPS work-related purposes. Occasional and reasonable personal use is tolerated provided that this does not interfere with the performance of your normal work duties or incur any cost to the IPS.

4.5.2 Users must ensure that they use ICT resources at all times in a manner which is lawful, ethical and efficient and does not interfere with the integrity or reputation of the IPS.

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

4.6 Monitoring

4.6.1 The IPS reserves the right to maintain and examine logs of any, or all uses of its ICT resources, in order to:

a) Prevent, detect or minimise inappropriate use.

b) Ensure compliance with IPS policies, current legislation and applicable regulations or policies.

c) Resolve technical issues with ICT equipment.

d) Ensure system performance and availability.

e) Protect the privacy and integrity of information stored on the IPS network.

f) Investigate suspected security incidents.

g) Protect the rights and property of the IPS, its employees and prisoners.

4.6.2 This monitoring may include, but is not limited to individual login sessions, contents of hard disks, internet sites visited, telephone usage and the content of electronic communications (email, instant messaging, fax)

4.6.3 The monitoring of an individual user's ICT activity must be authorised by the Director of Estates and ICT or the Head of ICT. The results of all monitoring will be stored securely for a specified period of time and will only be shared with those authorised to have access to such information.

4.6.4 To comply with Data Protection guidelines, monitoring data will only be collected and kept for as long as it is required and destroyed afterwards.

4.6.5 The IPS reserves the right to withdraw email, internet facilities or other telephony services from you at any time. As an ICT user you are expected to exercise good judgment and to act in a professional manner when accessing the internet or using email or other telephony services.

4.7 Confidentiality & Privacy

4.7.1 All data held on official computers is confidential to the IPS and must be treated in a manner that protects it from being inappropriately used or divulged. Data held on official computers is subject to the protection afforded by the Official Secrets Act, the Data Protection Act, the Freedom of Information Act and any other relevant legislation or policies.

4.7.2 In the course of a users work for the IPS, he/she may have access to, or hear information concerning the medical or personal affairs of a prisoner and/or employee's. Such information irrespective of the format is strictly confidential, must always be safeguarded and:

a) Users must respect the privacy and confidentiality of any information at all times and must not access information unless they have a valid IPS work-related reason or have been granted permission by the information owner.

b) Confidential or personal information must only be discussed or shared with other IPS employees and third parties who have a valid IPS work-related reason and are authorised to have access to the information.

c) If you are unsure whether you are authorised to divulge or pass on information to third parties, you should check with your Director/Governor, ICT or HR before passing on the information.

d) Information 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.

e) Users must not remove from their IPS employment location any confidential or personal information, (irrespective of the format - paper, electronic or otherwise) belonging to the IPS without the authorisation of the information owner.

f) In circumstances where a user is on-leave or out of the office, their line manager may be permitted subject to approval by their Director/Governor (and after permission from the Director of Estates and ICT or Head of ICT) to access their computer system to retrieve documents or emails necessary to deal with routine IPS work-related matters. In such circumstances line managers must respect the privacy of the individual user and not access documents or emails of a personal nature unless there are compelling conditions that warrant doing so (For example the detection and prevention of fraud).

g) Confidential or personal information must not be used for training, demonstration or research purposes unless it has first been anonymised. Only in exceptional circumstances (such as resolving production problems or carrying out UAT testing) should live data be used in a test environment. In such circumstances, the data must be kept protected on the test systems, particularly when its usage is no longer required.

4.8 Information Security

4.8.1 Information Security (commonly referred to as ICT Security) means protecting information and information systems from unauthorised access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction.

4.8.2 Information Security is primarily concerned with the confidentiality, integrity and availability of data regardless of the form the data may take: electronic, print or other forms.

4.8.3 In accordance with the provisions of the Irish Data Protection Acts 1988 and 2003, organisations such as the IPS that store personal information about its employees, clients and prisoners, have a legal responsibility to ensure the privacy and security of this information at all times.

4.8.4 Users must not discuss the security mechanisms employed by the IPS to protect its information with any unauthorised persons. Unauthorised persons are people who are not staff members of the IPS and staff members who are not authorised to use its ICT equipment.

4.8.5 Users must not attempt to deliberately disable or circumvent any security controls or procedures implemented by the IPS, e.g. tamper with locked down USB ports or CD/DVD drives.

4.8.6 IPS computer devices 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 screen.

4.8.7 Users should operate a clear screen policy. They must log off or 'lock' their IPS ICT device when they have to leave it unattended for any period of time and at the end of the each working day.

4.8.8 Users should operate a clear desk policy. At the end of each working day or when leaving their workplace for a major part of the day, users should clear their desks, and lock away all confidential or personal information (irrespective of the format - paper, electronic or otherwise).

4.8.9 Confidential or personal information, when printed, should be collected from printers, fax machines or multi function devices immediately.

4.8.10 Authorised removable storage devices should be stored away in a locked cabinet or drawer, when not in use.

4.8.11 Any user who discovers a "security hole" in any system allowing them to access information they are not authorised to, should report the incident to the IPS ICT Helpdesk.

4.8.12 Users must report all actual or suspected breaches of information security immediately to their line manager and to the ICT Section**.**

4.9 User Accounts & Passwords

4.9.1 Where technically feasible all IPS ICT resources must be password protected.

4.9.2 Where appropriate, individual users will be granted access to IPS ICT resources necessary for them to perform their specific duties for the IPS.

4.9.3 User access to the IPS ICT resources will be controlled by the use of unique user accounts and passwords. Users may receive multiple unique user accounts and passwords for access to different resources.

4.9.4 Users must only use user accounts and passwords which have been assigned to them.

4.9.5 The use of generic or group user accounts is strictly prohibited.

4.9.6 All user accounts must be created and managed by the IPS ICT Section.

4.9.7 Each user is responsible for all activities performed on any IPS ICT device, information system or application while logged in under their user account and password. This would be taken into account in the event of a security incident or investigation.

4.9.8 Users must ensure passwords assigned to them are kept confidential at all times and are not shared with others including their co-workers or third parties.

4.9.9 On rare occasions when users call the IPS ICT Helpdesk with a specific Lotus Notes issue, the ICT Helpdesk may ask for your Lotus Notes email password only. When the problem has been resolved, users should change their Lotus Notes password. Outside of this situation, if you are asked for any password, do not provide it and report the incident to the IPS ICT Helpdesk and to ICT management.

4.9.10 Staff and third parties working in a prison, who receive a password from their ICT Coordinator, must change it straight away, if not forced to do by the system.

4.9.11 When making a password reset request to the IPS ICT Helpdesk, the ICT Coordinators must ensure that the new password is securely communicated to the staff member or third party and not shared or given to anyone else.

4.9.12 ICT Coordinators must not log into any ICT system using another parties credentials that they may be aware of.

4.9.13 Users must not write down their password(s). In exceptional circumstances where a password has to be written down, the password must be stored in a secure locked place, which is not easily accessible to others.

4.9.14 Users must choose passwords that are difficult to guess and must never be left blank.

4.9.15 Where technically feasible, passwords must contain at least 8 characters, include a combination of letters (both upper & lower case), numbers (0-9) and at least one special character (for example: “, £, $, %, ^, &, *, @, #,?, !, €).

4.9.16 Passwords must be changed regularly e.g. at least every 90 days or when instructed.

4.9.17 No password should be re-used by a user within a 12 month period.

4.9.18 Where possible, user accounts should be set to lock-out after at least 5 unsuccessful login attempts.

4.9.19 Where possible, IPS systems should force users to change passwords after first logon. Where this is not possible, they should be instructed to manually do so.

4.9.20 Where possible, IPS systems will be set by ICT to “log out” users after at least 15 minutes of inactivity. Where this is not possible, users must manually log off or ‘lock’ their IPS computer device (using Ctrl+Alt+Delete or ‘Windows’ key + L’) when they have to leave it unattended for any period of time and at the end of the each working day.

4.9.21 Users must not send their passwords within email messages unless the email message is encrypted. Seek advice from the ICT Helpdesk on how to do this if needed.

4.9.22 Passwords must not be stored electronically in clear text.

4.9.23 Users who suspect their password is known by others must change their password immediately.

4.10 Software & Electronic Media

4.10.1 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. Users should be aware that copyrighted material can be those that include software, text, picture, video and music.

4.10.2 Only software which has the correct and proper license and has been purchased and/or approved by the IPS ICT Section may be installed and used within the IPS.

4.10.3 Software and electronic media should only be installed on official IPS computers by ICT personal.

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

4.10.5 The IPS ICT Section on behalf of the IPS reserves the right to remove software at any time.

4.11 ICT Computing Devices

4.11.1 All IPS ICT equipment/software (no matter how small) must be purchased through an existing ICT Framework Agreement in conjunction with the ICT Section. Any intended purchase of IPS equipment/software that is not through the agreed channels must be approved either by the Head of IPS ICT or Director of Estates and ICT before they are purchased and connected to the network or other IPS equipment.

4.11.2 Users can only connect official IPS ICT computing devices to the IPS network after receiving prior authorisation from the IPS ICT Section.

4.11.3 Users can only connect another IPS ICT computing device to their local computer after receiving prior authorisation from the IPS ICT Section.

4.11.4 Users cannot alter the hardware or software configuration of their ICT computing device without prior authorisation from the IPS ICT Section.

4.11.5 Users cannot connect or disconnect any IPS ICT computing devices to or from any IPS network without prior authorisation from the IPS ICT Section.

4.11.6 All ICT computing devices provided by the IPS remain the property of the IPS.

4.11.7 Users must not remove or borrow IPS ICT computing devices without the authorisation from IPS ICT Section.

4.11.8 The overall security and responsibility of the borrowed devices is the responsibility of the borrower and must be returned to IPS ICT Section before they leave the employment of the IPS or at the request of the borrower's line manager.

4.11.9 Users must take reasonable steps to ensure that no damage is caused to their IPS issued ICT computing device.

4.11.10 If an IPS ICT computing device is lost or stolen and contains confidential or personal information, this must be reported to the IPS ICT Helpdesk immediately who will then report the matter to the Data Protection Commissioner as a potential security breach.

4.11.11 Each user is responsible for all activities performed on any IPS ICT computing device, information system or application while logged in under their user account and password.

4.12 Mobile Computer Devices

4.12.1 Mobile computer devices apply to all mobile computing equipment that is owned, rented or leased by the IPS. Mobile computing equipment may include but is not limited to:

a) Laptops

b) Tablets (e.g. Apple iPads)

c) Ultra books (combined tablet and laptop)

d) Smartphone's (e.g. Blackberry, Apple iPhone)

e) Any other form of Personal Digital Assistants (PDAs)

4.12.2 Mobile computing facilities will only be provided to a limited number of staff members that are authorised by their line manager and Director of Estates and ICT.

4.12.3 BYOD (Bring Your Own Device) and the use of personal mobile computing devices for official prison duties are strictly prohibited by the IPS ICT Section.

4.12.4 Users of official mobile computer devices must take all reasonable steps to prevent damage or loss to the mobile computer device.

4.12.5 Users of mobile computer devices must ensure that the security mechanisms applied to them by the IPS are not tampered with or circumvented.

4.12.6 Smart devices (Tablets and Smartphone's) are potentially at risk to infection by malicious software such as virus and malware and can propagate though the use of rogue apps, malicious websites and e-mail.

When using IPS Smart devices, users must only install apps from official app stores provided by the mobile vendor (e.g. Apple, Google, Microsoft, and Blackberry) or from the IPS internal app store, if one is provided.

4.12.7 Users should be vigilant and apply good judgment when installing apps on IPS Smart devices as they can require a certain level of security permissions on the device when installed e.g. an alarm clock app that wants to read your contacts and text messages should be treated with extreme caution!

4.12.8 IPS ICT reserve the right to monitor usage of IPS provided Smart devices and restrict their usage and functionality as appropriate.

4.12.9 All mobile computer devices must be password protected in accordance with the User Account and Password guidelines set out in this document. This includes applying a password to both the device itself and the SIM card.

4.12.10 Confidential or personal information must only be stored on an IPS mobile computer device with the authorisation of the information owner and IPS ICT. 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 personal information must be stored on the IPS mobile computer device as is absolutely necessary for a given function to be carried out and securely deleted when finished with.

4.12.11 When working in the office, mobile computer 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, they should be secured to a desk using an appropriate locking mechanism (i.e. cable lock) or, locked in a drawer or filing cabinet.

4.12.12 Mobile computer devices must not be left unattended when working off-site.

4.12.13 When travelling by car, IPS mobile computer devices should be stored securely out of sight, when not in use. Avoid leaving mobile computer devices unattended in the boot of a car overnight.

4.12.14 When travelling by taxi, train or plane, IPS mobile computer devices should be kept close to hand at all times. Avoid placing the mobile computer device in locations where they could easily be forgotten or left behind.

4.12.15 The use of IPS mobile computer devices should only be used when it is safe and appropriate to do so and abides by the law e.g. do not use when driving (unless with the use of an official hands-free kit) or in areas where mobile devices should be switched off.

4.12.16 When using an IPS mobile computer device in a public place, users need to take precautions to ensure the information on the screen cannot be viewed by others.

4.12.17 If using public Wi-Fi access points or hotspots, prefer WPA-encrypted hotspots to WEP and unsecure Wi-Fi. If you have to use untrusted internet hotspots, avoid using ones with common names such as “Free Wi-Fi”, as these are quite possibly maintained by a hacker who would gain full visibility of your traffic. Limit the amount of activity on untrusted networks e.g. avoid carrying out Internet banking and other highly confidential transactions.

4.12.18 Blindly connecting to unencrypted access points can let your phones leak all sorts of useful things for malicious actors to intercept and act upon. Set your smart device to forget networks you no longer use, so as to minimise the amount of data leakage and configure your phone to automatically turn on/off wireless in certain places using a location-aware Smartphone app.

4.12.19 Ensure you are familiar with the Bluetooth settings on your mobile computing device in order to prevent unauthorised users connecting to it via the Bluetooth interface. At a minimum, you must adhere to the following guidelines.

a) Do not accept pairing requests from devices you do not recognise.

b) Due to the security weaknesses in some versions of Bluetooth, it must not be used to transfer IPS confidential or personal information between devices or used to make confidential phone conversations, unless you are in an isolated environment free from potential eavesdropping.

c) Ensure that the Bluetooth interface is turned-off on your mobile computer device when Bluetooth is not required.

d) Ensure that your mobile computer device is not set to be discoverable by Bluetooth.

e) Ensure that you use a strong pairing password when pairing Bluetooth enabled devices and not use a common default of 0000.

4.12.20 Users must not use their IPS mobile computing device as a "Mobile Hotspot" to provide shared internet access to other client devices, a feature known as "tethering". This could result in very large data charges, especially if roaming abroad.

4.12.21 If using web based or client software for e-mail access, connect securely using SSL encryption.

4.12.22 Users must ensure that all IPS mobile computer devices provided to them are not accessed (including internet access) by persons who are not IPS employees.

4.12.23 Remote access connections to the IPS network, from an IPS mobile computer device must be made in accordance with IPS Remote Access procedures.

4.12.24 All users of mobile computing devices with integrated telephone and video features must follow common sense usage. These include but not limited to

a) Familiarising themselves with the safety and operating instructions contained in the operators manual

b) Not using the device while driving.

c) If a car kit is in use, be alert to the environment around you.

d) Limiting usage to only official business purposes.

e) Not using profane, abusive, derogatory or obscene remarks in any communications whatsoever.

f) Not using video and sound recording capability to record and store images and sounds that will infringe on the privacy of others or compromise the security or reputation of the IPS.

4.12.25 Users that use mobile computing devices for electronic communications such as e-mail, instant messaging and Internet must also adhere to usage policy set out in this document.

4.13 Email & Instant Messaging

4.13.1 The IPS email system is provided to staff for business use and to promote effective communication on IPS business matters. The policies in this document apply equally to instant messages and email on IPS approved platforms (e.g. using Cisco Unified Personal Communication/Jabber and Outlook or Lotus Notes).

4.13.2 Only official IPS email & instant messaging software must be used on ICT computing devices.

4.13.3 All email & instant messaging communication on IPS computers and networks are legally the property of the IPS and should not be regarded as entirely private.

4.13.4 Personal email & instant messaging must be kept to a minimum. Occasional and reasonable personal use is tolerated provided that:

a) This does not interfere with the performance of your normal duties or with the integrity of the IPS email system.

b) the systems are not used for private business or other commercial purposes, including the sale or purchase of goods or services.

c) Personal communication must be presented in such a way that is clear to the recipient that the email is personal and is not communicated on behalf of the IPS.

d) there is no breach of the prohibitions contained in this policy.

4.13.5 Only email & instant messaging facilities provided by the IPS may be used in connection with an individual users work for the IPS. The use of third party or web based email & instant messaging accounts for the transmission of IPS information is strictly prohibited.

4.13.6 Where it is necessary to transmit confidential or personal information to an email addresses outside of the IPS (one that does not end in "@irishprisons.ie"), the following additional procedure must be followed

a) The transfer must be authorised by the information owner/Governor/Director/IPS ICT.

b) All confidential or personal information sent with the email message must be encrypted inline with the requirements of the IPS encryption procedures. Please contact the IPS ICT Helpdesk for assistance.

c) The password used to decrypt (read) the confidential or personal information must not be sent along with the original email message.

4.13.7 Do not send any material which may be offensive or disruptive to others or which may be construed as harassment, sexual harassment or bullying

4.13.8 Do not send emails containing comments that are defamatory, insulting or harassing, or remarks that could be offensive to others such as comments including but not limited to race, religion, sexual orientation, gender or age. Be aware of IPS core values and policies.

4.13.9 Even though the IPS employs anti-virus and anti-spam software, some virus infected messages can enter the company's messaging systems. Viruses, "worms" and other malicious code can spread quickly if appropriate precautions are not taken and you must therefore adhere to the following guidelines:

a) Be suspicious of messages sent by people not known by you.

b) Do not launch, detach or save any executable file (i.e. those ending in ".exe" or ".vbs") under any circumstances. Contact the IPS ICT Helpdesk immediately upon receipt of such an e-mail.

c) Do not open, detach or save any unofficial file attachments to your hard disk or any network drive. Official attachments should be placed in the relevant document library or hard copy file.

d) Do not instigate or forward chain letters or "junk mail". Simply delete them.

e) Do not send any unofficial graphics or executable files

f) Do not instigate or forward "junk mail" to other users internal or external

g) Do not, under any circumstances impersonate any other person when using email & instant messaging and do not attempt to amend a message received without the prior approval of the author.

4.13.10 All email & instant messaging may be recoverable, even if you have deleted them.

4.13.11 Email & instant messaging carries the same legal status as other written documents and should be treated with the same care.

4.13.12 In relation to the retention of all work-related records created by them, email & instant messaging which are of "enduring organisational interest" are records under the Freedom of Information and Archive Acts and must not be solely kept in your e-mail account. They must be transferred to the appropriate document library and/or hard copy file. Regardless of where they are stored, they are records for the purposes of the Freedom of Information and Data Protection Acts, and must be considered for release should a request for the records be received. Only records in existence on the date of an application under the aforementioned legislation may be considered for release to the applicant.

4.13.13 The amount of email in a user's personal inbox and sent items folder must be kept to a minimum. Personal emails and attachments that are not work-related must be deleted as soon as possible after receipt.

4.13.14 Old IPS work-related email and attachments that are no longer required should be deleted and those that need be retained should be archived.

4.13.15 Consider compressing large attachments such as tender documents, drawings, large photographic files before sending by email. Please contact the IPS ICT Helpdesk for assistance with this, if required.

4.13.16 Do not auto forward IPS emails to another recipient email address.

4.13.17 Do not auto forward personal emails to your IPS email address.

4.13.18 A disclaimer will be automatically attached to all out-going email messages by the IPS email system. This disclaimer does not excuse the user from undertaking fundamental checks before sending the email (i.e. checking the email content for accuracy, correct address etc.)

4.13.19 Be vigilant when sending emails to ensure that the recipient email address(s) are correct. Emails once sent are sent and in all likelihood will be read by the recipient.

4.14 Internet & Intranet

4.14.1 The primary purpose of the IPS internet and intranet service is to provide access to a valuable business tool to facilitate communication, education and learning, information sharing and authorised research.

4.14.2 The use of the internet facilities for personal reasons must be kept to a minimum and adhere to the requirements of this policy.

4.14.3 In accordance with the IPS Internet Content Filter policy, the IPS automatically filters access to categories of internet content that it considers inappropriate, e.g. gambling and pornography.

4.14.4 The IPS ICT Section may block access to sites/material which it considers may compromise the security of the IPS network.

4.14.5 Do not deliberately visit, view, or download any material from any website containing sexual or illegal material or material which is potentially offensive in any way.

4.14.6 The IPS content filtering system records all sites visited by users and reserves the right to inspect these audit trails periodically. The IPS will keep a record of a user's web browsing activity for a specified period of time including sites visited.

4.14.7 In circumstances where a user has a legitimate IPS work-related reason to access filtered internet content, they may, with the approval of their line manager request access to such content for a specified period of time. Access requests must be submitted in writing using the IPS ICT Helpdesk and supported by a business case approved by your Director/Governor.

4.14.8 Confidential information regarding IPS business practices and procedures or personal information about any prisoners, clients or employees should not be published on the IPS internet site (www.irishprisons.ie) or intranet site (http://iris).

4.14.9 Confidential or work related information regarding IPS business practices and procedures or personal information about any prisoners, clients or employees must not be posted or discussed on social networking websites (e.g. Facebook, Twitter and LinkedIn), internet video hosting/sharing websites, internet discussion forums, message boards or internet chat rooms. Please refer to IPS Social Media Policy for more information.

4.14.10 Confidential or personal information must only be transmitted via the public internet when the information has been encrypted and the transfer has been authorised by the information owner and the ICT Section. Please contact the IPS ICT Helpdesk for assistance with this, if required.

4.14.11 Users should be aware that information hosted on the internet offers no guarantee of accuracy, reliability or authenticity.

4.14.12 Users should not use IPS information to subscribe for non-business purposes to Web 2.0 and social media sites, external bulletin boards, newsgroups or any other internet service without prior written permission of the ICT Section. This includes using IPS e-mail addresses, IPS contact telephone/fax numbers or postal addresses.

4.15 Fax & Printing

4.15.1 The policy on fax and printing applies regardless of the type of device used e.g. standalone fax/printer or multi-function device (Combined Fax, Printer, Scanner, and Copier).

4.15.2 Users who receive fax messages where they are not the intended recipient must contact the sender and notify them of their error.

4.15.3 Users must respect the privacy of others and only access fax messages where they are the intended recipient or they have a valid IPS work-related reason.

4.15.4 In circumstances where confidential or personal information is sent by fax, the following procedure must be followed:

a) The fax message must include an official IPS Fax Cover Sheet where one is provided.

b) Only the minimum amount of confidential or personal information should be included in the fax message as is necessary for a given function to be carried out.

c) Before sending the fax message, the sender must contact the intended recipient to ensure he/she is available to receive the fax within an agreed timetable.

d) The sender must ensure that fax number dialed is correct.

e) When the fax message has been sent, the sender must keep a copy of the transmission slip and contact the intended recipient to confirm receipt of the fax message.

f) The sender must ensure that no copies of the confidential fax message are left on the fax machine.

4.15.5 Only fax machines and printers which are owned or leased by the IPS should be used to send or receive fax's or print confidential or personal information

4.15.6 All transfer of confidential or personal information via fax message to third parties must be authorised by the information owner.

4.15.7 Fax machines which are used to send or receive confidential fax messages must be physically secured and positioned in such a way as to minimise the risk of unauthorised individuals accessing the equipment or viewing any incoming messages. Where possible, the fax machine should be switched off outside of normal office hours.

4.15.8 Fax messages are capable of forming or varying a contract in the same way as a written letter. Users must be careful when wording a fax message, so it cannot be construed as forming or varying a contract when this is not the intention.

4.15.9 Fax messages carry the same legal status as other written documents and should be used with the same care. Fax communications maybe subject to Freedom of Information Act and therefore available for public distribution.

4.15.10 Users must take care when printing confidential or personal information on IPS printer's e.g**.**

a) When sending confidential or personal information to a printer, ensure that the intended printer is correct.

b) Remove the printed material immediately after the job has finished.

c) If you find that you have printed confidential or personal information to the incorrect printer, don't ignore it, please follow up to ensure that the information is removed from the printer immediately.

d) If you find unclaimed material lying around the printer/fax, please discard it appropriately if an owner cannot be found.

e) In IPS departments where a secure fax/printing solution has been implemented, do not share your device credentials with anyone e.g. pin number or swipe card.

f) If you are unsure how to cancel a print job, change printer settings or cannot physically locate a printer in the building, please contact the IPS ICT Helpdesk immediately.

4.16 Telephone & Mobile Phone

4.16.1 This policy applies to all land line phones supplied to staff and to those mobile phones issued by the ICT Section including mobile phone accounts required to support mobile communications devices such as iPhone, Android, Windows Phone etc.

4.16.2 All phones, whether land line or mobile, will remain the property of the IPS and an account will be discontinued where the IPS ICT Section is not satisfied that its usage is in keeping with this policy or the IPS requirements generally.

4.16.3 Land line and mobile phones are issued for IPS business call purposes. You should have regard to value for money and adopt a sensible approach in their usage. Where convenient to do so, landlines should be used instead of mobile phones and unnecessary usage while abroad should be avoided.

4.16.4 Phones should not be used to harass or defame, or to send obscene or offensive messages/pictures.

4.16.5 A modest amount of personal usage is tolerated. The IPS ICT Section reserves the right to monitor phone usage and routinely refer accounts above average usage levels to users for confirmation that the usage was predominantly official. The user may be required to reimburse IPS for the cost of personal calls where this is not the case.

4.16.6 You should take normal common-sense precautions to prevent loss, misuse or theft of any mobile phone issued to you. In the event that an official mobile phone is lost or stolen, the user must contact the IPS ICT Helpdesk immediately to block the account and void the phone.

4.16.7 An official mobile phone should never be left unattended such that it might be used by others.

4.16.8 All mobile phones must be password protected in accordance with the User Account and Password guidelines set out in this document. This includes applying a password to both the device itself and the SIM card.

4.17 Information Storage

4.17.1 Where possible, all confidential information, personal information and IPS information systems that store or process such information must be stored/hosted on a secure IPS network server.

4.17.2 In circumstances where the technical or business requirements necessitate, the Director of Estates and ICT or the Head of ICT may approve the storage/hosting of confidential information other than on an IPS network server. In such circumstances the information owner and user of the IPS computer device have a responsibility to ensure

a) Only the minimum amount of confidential or personal information that is necessary for a specified task is stored on the computer device.

b) The ICT computer device is password protected.

c) The confidential or personal information, and/or the computer device are encrypted.

d) The confidentiality and privacy of the information is maintained at all times and is only accessible to the authorised user of the computer device.

e) The computer device is regularly backed up, and the backup copies are stored in a secure place and not with the computer device.

f) At the completion of the task, all copies of the confidential or personal information stored on the computer device are permanently deleted.

4.17.3 The hosting/storage (temporary or long term) of IPS information systems, confidential or personal information (encrypted or otherwise) on USB flash drives (i.e. memory stick/pen/keys) is strictly prohibited.

4.17.4 IPS employees are strictly prohibited from hosting/storing IPS information systems, confidential information on any computer device, mobile computer device, mobile phone device or removable storage device which is their personal property and is not owned or leased by the IPS.

4.17.5 IPS network servers are reserved for the hosting/storage of IPS work-related systems and information only. Users must store all non work-related information belonging to them on their local IPS computer device.

4.17.6 The hosting/storage/transfer of IPS digital confidential information by any third party must be authorised by the Director of Estates and ICT or the Head of ICT.

4.18 Information Backup

4.18.1 IPS network servers will be automatically backed up on a daily basis.

4.18.2 Users who do not have access to an IPS network server must ensure that they regularly backup all their important information onto another computer or approved removable storage device. Each user is responsible for ensuring their backup information is kept safe and secure.

4.18.3 Information backups especially those containing confidential or personal information must be stored securely in a locked drawer, filing cabinet or safe.

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

4.18.5 Confidential or personal information must not be backed up on personal memory USB flash drives (i.e. memory stick/pen/keys).

4.18.6 Where USB memory sticks are used – only authorised encrypted USB memory sticks may be used for official purposes. Users must ensure that a complex password as recommended is this document is utilised.

4.18.7 The use of cloud based services such as iCloud, Drop box, Google Drive etc. is strictly prohibited for the storage and backup of IPS confidential, personal and private company information.

4.19 Information Transfer

4.19.1 All transfer(s) of confidential or personal information to third parties must be made in accordance with the Irish Data Protection Act 1988 and 2003.

4.19.2 All transmission of confidential or personal information through a public network (for example the internet) to external third parties must be authorised by the information owner, Director of Estates and ICT or the Head of ICT. The information must be encrypted or be transmitted through an encrypted tunnel (for example a secure Virtual Private Network (VPN) Secure Sockets Layer (SSL) or Secure FTP).

4.19.3 All confidential or personal information transmitted around wireless networks must be encrypted using WPA2 (Wi-Fi Protected Access) or better.

4.19.4 Only the minimum amount of information must be transferred as is necessary for a given task to be carried out.

4.19.5 Where possible all transfer(s) of confidential or personal information must be carried out electronically and in line with the IPS email guidelines.

4.19.6 In exceptional circumstances, confidential or personal information maybe transferred manually using an IPS approved removable storage device .This ensures that the confidential or personal information is encrypted and password protected.

4.19.7 The removable storage device must wherever possible be accompanied by an IPS employee, and delivered directly to and signed by the intended recipient.

4.19.8 Contact the IPS ICT Helpdesk for information on approved removable storage device usage.

4.20 Information Disposal

4.20.1 Confidential or personal information must be securely deleted when it is no longer required.

4.20.2 All traces of the information must be removed from old computers, mobile computer devices, mobile phone devices and removable storage devices before they are reused within the IPS, sold to employees, donated to charity, or recycled.

4.20.3 The simple deletion or formatting of information is not sufficient to remove all traces of the information. The information must be overwritten using special sanitation software which is available from the IPS ICT Section or the computer device used to store the information must be physically destroyed.

4.20.4 The IPS ICT Section has facilities to professionally delete and destroy information on hard drives, USB memory sticks, DVD's, CD's and other storage media. If you wish to dispose of these devices and devices such as old PC's, laptops, printers etc, you must contact the ICT Help Desk who will assist.

4.20.5 Hardcopies of confidential or personal information must be destroyed in a paper shredder or placed in a confidential waste bin.

4.21 Enforcement

4.21.1 The IPS reserves the right to take such action as it deems appropriate against users who breach the conditions of this policy. IPS employees who breach this policy may be denied access to the IPS ICT resources and maybe subject to disciplinary action in accordance with the Prison (Disciplinary Code) Rules 1996 for Prison Officers or the Civil Service Code of Discipline for civilian Prison based staff, or any legislation superseding these documents.

4.21.2 The viewing, downloading or distribution of offensive material is strictly prohibited and as such will be subject to disciplinary action in accordance with the Prison (Disciplinary Code for Officers) Rules 1996 for Prison Officers or the Civil Service Code of Discipline for civilian Prison based staff, or any legislation superseding these documents.

4.21.3 The nature of any breach of this policy will dictate the appropriate disciplinary action to be taken and each case will be considered on its merits and processed in accordance with the Disciplinary Procedures.

4.21.4 Breaches of this policy by a third party, may lead to the withdrawal of IPS ICT resources to that third party and/or the cancellation of any contract(s) between the IPS and the third party.

4.21.5 The IPS will refer any use of its ICT resources for illegal activities to the appropriate law enforcement agencies.

4.22 Review and Update

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

4.22.2 ICT and/or SCS will communicate any changes to policy however it is advised that you regularly check the Intranet (IRIS) and review the most up to date version of this policy and all other related ICT policies. http://iris/Pages/default.aspx

4.22.3 It is the responsibility of each individual user to familiarise themselves with the latest version of this policy. Failure to do so does not exempt users from their obligations under this policy.

4.23 References

Information and Communications Technology Acceptable Usage Policy, Department of Justice and Equality

Protecting the confidentiality of personal data - guidance note, CMOD, Department of Finance, Dec 2008

http://www.dataprotection.ie/documents/guidance/GuidanceFinance.pdf

5. Related Policies and Legislation

PIN 026 Irish Prison Service Social Media Policy

The Official Secrets Act 1963.

The Data Protection Acts 1998 and 2003,

The list of all relevant Legislation and Acts are listed in Appendix II

6. Definitions

A list of terms used throughout this policy is defined in Appendix I.

Appendices

Appendix I – Definitions

Appendix II – Irish Legislation and Acts

Appendix I – Definitions

Anonymised	Anonymised data is information which does not identify an individual directly. Anonymisation requires the removal of an individual's name, address, date of birth, PPS number and any other combination of details that might support identification.
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.
Bluetooth	Bluetooth is a wireless connection which can be used to transfer files between two devices or to establish a connection to other devices, such as a wireless headset or keyboard.
Breach of Information Security	The situation where IPS confidential or personal 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.
Computer Virus	A computer virus is a computer program that can replicate itself and spread from one computer to another. It is also used to refer to other types of malware programs that do not have a reproductive ability such as adware and spyware programs. A computer virus generally attaches itself to an existing program and almost always corrupts or modifies files on a targeted computer.
Computer Worm	A computer worm is a standalone malware program that replicates itself in order to spread to other computers. It often uses a computer network to spread itself, relying on security failures on target computers to access it. Unlike a computer virus, it does not need to attach itself to an existing program and generally consumes network bandwidth.
Confidential Information	Information that is given to IPS in confidence and/or is not publicly known. The Information must only be accessible to those person(s) who are authorised to have access. For example – unpublished financial reports, tenders, contracts, unpublished research material, passwords etc.
Encryption	In cryptography, encryption is the process of obscuring information to make it unreadable without special knowledge. For example having access to a password or secure key to decrypt the information.
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.
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 an IPS directorate.
Information and Communications Technology (ICT) resources:	Includes all computer facilities and devices, networks and data communications infrastructure, telecommunications systems and equipment, internet/intranet and email facilities, software, information systems and applications, account usernames and passwords, and information and data that are owned or leased by the IPS
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.
LAN (Local Area Network)	A computer network that interconnects computers in a limited area such as an office building. LAN networks have high data speeds and do not depend on third party telecommunications lines.
Malware	Malware (short of malicious software) is used or created by attackers to gather sensitive information, gain access to computer systems or disrupt computer operations. Malware is a general term used to refer to a variety of forms of hostile or intrusive software. Malware includes computer virus, computer worms, trojan horses, most root kits, spyware, dishonest adware and other malicious or unwanted software.
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, 3G/GPRS mobile data cards. This does not include cordless telephones which are an extension of a telephone physically connected to a landline telephone system.
Personal Information	Information relating to a living individual (i.e. IPS employee, client or prisoner) 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 the IPS Information and Communications Technology (ICT) resources for any activity(s) which is not IPS work-related.
Privacy	The ability of an individual or group to seclude themselves or information about themselves from being made public. They wish to remain unnoticed or unidentified in the public realm.
Removable Storage Device	Any optical or magnetic storage device or media, including but not limited to CD, DVD, Blue-Ray, floppy disks, magnetic tapes, ZIP disk, Memory cards (i.e. memory stick/flash/SD), external/portable hard drives.
Rootkit	A rootkit is a stealthy type of software used by hackers and designed to hide the existence of certain processes or programs from normal methods of detection and enable continued privileged access to a computer.
Spyware	Spyware is software that aids in gathering information about a person or organization or assert control over a computer without their knowledge or consent.
Trojan Horse	In computing terms, a Trojan is a non-self-replicating type of malware which appears to perform a desirable function but instead facilitates unauthorised access to a computer system. Trojan horses may steal information or cause harm to a computer. Trojan horses may be installed as part of downloaded software such as online games.
WAN (Wide Area Network)	A network that covers a broad area that links across regional or national boundaries using private or public networks.

Appendix II – Irish Legislation and Acts

- The Data Protection Act, 1988 (Amendment Act 2003)
- The Copyright and Related Rights Act 2000 (Amendment Act 2004 and 2007)
- The Freedom of Information Circular 7/98 and Acts 1997 and 2003
- The Criminal Damages Act 1991
- The Official Secrets Act 1963
- Rules for the Government of Prisons 1947 (and various amendments)
- The Criminal Evidence Act 1992
- Section 9 of the Criminal Justice (Theft and Fraud Offences) Act, 2001
- Offences against the State (Amendment) Act 1998
- Child Trafficking and Pornography Act 1998
- Human Rights Commission Act, 2000 (Amendment Act 2001)
- Postal and telecommunications Services Act 1983 (Amendment Act 1984, 1999)
- Post Office (Amendment) ACT 1951
- The Defamation Act 1961
- Section 23 (Defamation) of the Electronic Commerce Act, 2000
- Employment Equality Act 1998
- Article 40.3.2 of the Irish Constitution regarding defamation
- Article 8 of the European Convention on Human Rights
- Public Service Management Act 1997
- Civil Service Code of Standards and Behavior Circular 26/2004 and Standards in Public Office Act 2001
- Civil Service Disciplinary Code Circular 14/2006 and Civil Service Regulation (Amendment) Act 2005

- Civil Servants and Politics Circular 21/1932
- Use of influence by Civil Servants Circular 17/1932
- Civil Servants and outside occupations Circular 16/1936
- Dealing with the Public Circular 32/1997
- Approved EU directives

All above acts can be found at http://www.irishstatutebook.ie

END OF DOCUMENT