Prisoner internet access

Policy Document

Policy Index No.	Policy Sponsor	Page/s	Approved by	Date
025	Care and Rehabilitation Directorate	5	Director of Care and Rehabilitation	15/06/15

Related policies/standards	Date
Prisoner internet access protocol LP/11/025-P1	15/06/15

Legacy reference of policy	Date for review of policy	Date of issue/amendment
	15/06/2017	15/06/2015

IPS Policy for prisoner internet access

Table of Contents

1. Aim of this policy

1.1 To enhance the delivery of education services to prisoners.

1.2 To allow supervised, controlled and monitored prisoner access to the internet subject to the security exigencies of the Prison Service and public safety.

2. Purpose of this policy

2.1 To ensure the development of our education service is in line with modern developments and best practice.

2.2 To ensure prisoners are adequately prepared for the transition from custody to community by providing a model of service delivery which complements that used by community based agencies.

3. Scope of this policy

3.1 The policy covers all pre-approved prisoners and their teachers.

4. Procedures for implementation

4.1 Principles

The provision of education in prisons is regarded by the Irish Prison Service as a key element in the process of normalisation and rehabilitation of prisoners. Education helps a prisoner cope with imprisonment, facilitates their personal development, helps prepare for life after release and may create the conditions necessary to establish the appetite and capacity for lifelong learning.

4.2 Prisoner categories

This policy allows for access by all prisoner categories with the following exceptions:

4.2.1 Those convicted of offences involving offences against children, indecent images of children, child pornography and/or child prostitution and/or any indecency directed against children,

4.2.2 Those convicted of offences involving possession of extreme pornographic images, e.g. images portraying a threat to life, serious injury of a sexual nature, a human corpse or bestiality,

4.2.3 Those convicted of offences of a sexual nature where internet access was an element of the crime,

4.2.4 Those not found suitable following consideration by prison management,

4.2.5 In any event, the Minister will be the final arbiter as regards the extension of this facility to any prisoner.

4.3 Site content

Only those sites deemed appropriate and necessary will be made accessible to prisoners.

4.3.1 Educational sites that permit read only access to their discussion and tutorial forums will be made accessible,

4.3.2 Open University coordinators will liaise with tutors and make submit assignments on behalf of prisoners.

4.4 Supervision

A prisoner may apply for school and if deemed suitable following interview can be approved for access to the internet. The head teacher will apply to ICT for a unique prisoner log on code to allow internet access. All such requests must be copied to the Governor. If management disapproves, the process will be terminated.

4.4.1 The head teacher (or a teacher acting on behalf of) will be responsible to ensure that all participating prisoners sign the IPS computer policy user's agreement in advance. The head teacher will retain a copy of the signed user agreement,

4.4.2 The supervision and monitoring of prisoners during their time in the education unit and using the internet will be carried out by the teachers, subject to available resources.

Each prisoner's log on code or password will be related to his or her name which will enable teachers to monitor usage. Teachers will be supplied with a custody list at the start of each school day to aid this process. The use of id cards by prisoners will assist teachers to ensure only those prisoners listed for school time are in the education unit,

4.4.3 Prisoners will be allowed to use memory sticks. Memory sticks will be held by teaching staff and issued and collected at the start and finish of lessons. Only memory sticks issued by the education unit can be used in class. In the event of a memory stick going missing, the head teacher will inform the governor immediately,

4.4.4 Specialist software will be utilised to enable remote monitoring and spot checks on internet usage by prisoners,

4.4.5 A passive monitoring system will raise an alert if a prisoner accesses an unapproved site.

4.5 Availability

Prisoners will only be allowed to access to the internet during school times and at times when supervision and monitoring is available.

4.5.1 Prison management will be responsible for informing teaching staff if any particular prisoner is not to be allowed access to the internet.

4.6 Sanctions

If a prisoner defaults on the agreement he/she will not be permitted internet access or be considered for re admission to the programme for 4 weeks and only then following the express approval of the governor.

4.7 Prisoner transfer/release procedures

When prisoners are released or transferred, prison management will immediately send a request to ICT for web access to be terminated.

5. Definitions

ICT – the ICT section of the Irish Prison Service

6. Related Policies/Documents

Prisoner internet access protocol LP/11/025-P1 15/06/2015

Appendix I User contract form

Computer Use, Access and Security Rules for prisoners

Purpose of this document

To state the standards of behaviour, interaction with and use of the computer facilities expected from users in order to protect the equipment and the data held on the network and to protect the reputation of the Irish Prison Service and its staff. Failure to comply with these rules may result in disciplinary procedures being imposed under the 2007 Prison Rules and/or criminal prosecution.

1. **General**

If a user finds a way to bypass or circumvent any of the security or access arrangements he or she must inform a member of staff immediately. Any deliberate breach of these Rules or other Irish Prison Service regulation or any attempt to bypass or circumvent the IT security or access arrangements will be treated as misbehaviour. The equipment, the network and the systems running on the network should only be used in the manner intended and as directed by staff.

A user is responsible for anything that is done in any of his/her user accounts. You must protect yourself by protecting your user accounts, therefore: Don't use somebody else's account and do not let somebody else use your account.

Logging on via the Network Username and Password is the only way in which computers are to be used. Any attempt to circumvent these arrangements will be viewed as misbehaviour.

Any attempt to circumvent the disabling of external drives or ports (e.g. USB, CD, DVD, Floppy) will be viewed as misbehaviour.

Users must exit all systems and log out of the network when they are finished using a computer. This is an important security precaution. It is also a useful way to protect yourself as systems have an audit trail which records transactions made against the username of the person logged in when the transaction is made. Remember, you are responsible for activity that takes place using your accounts.

Under no circumstances should a user open the casing on a PC or server or remove any part from same or interfere with or remove any part from any cabling, switch, router, UPS or any other IT equipment. There should be no circumstances where this is necessary and to do so will be regarded as misbehaviour.

The viewing, downloading or distribution of offensive material is strictly prohibited and as such will be deemed as misbehaviour.

2. **Passwords**

Passwords must be used in conjunction with all accounts and should be kept secret at all times.

You are responsible for the use of the facilities granted in your name and your main protection is your password(s). Make them difficult to guess and above all, do not share your password with anyone or write it down. If you think someone knows your password, inform a member of staff as soon as possible.
Maintaining the privacy of your password is your responsibility and consequently you are responsible for any misbehaviour that takes place using your name and password. Do not leave your computer unattended without securing the session by password or logging off.

3. Use of Official Equipment

All IT software and equipment (Servers, PCs, printers, network kit and associated cabling and other IT infrastructure) is provided for official use only. This stipulation is meant to protect the equipment, the network and, most importantly, the data on the network. The equipment should be treated with respect and handled appropriately at all times in a manner which avoids the equipment being damaged. Do not to move PCs or printers from the location where they are originally set up.

4. Unauthorised Software

Only software purchased through IPS ICT Section and loaded onto official computers by personnel authorised to do so by the IPS ICT Section should be used. Do not load any other software onto official computers nor should you use such software. Use of unlicensed or unauthorised software has the potential to cause damage to the data held on the network. It is also illegal and may result in criminal prosecution.

5. Security

Bypassing the Prison Service computer network security by accessing the Internet directly by modem or other means is strictly prohibited and will be regarded as serious misbehaviour.

_____

I have read the rules detailed above and understand it is my responsibility to abide by them.

Name (please print in capitals)_____

PIMS No. _____

Prison/Place of Detention_____

Signature_____ **Date**_____

END OF DOCUMENT