11.7	USE OF INTERNET AND EMAIL

Applies to: Staff,	**Version: 1**
Specific responsibility: Office Manager, HECIS Co-Ordinator	**Date approved: 5.8.14**
	Next review date: Aug 21

Policy context: This policy relates to	
Standards or other external requirements	
Legislation or other requirements	
Contractual obligations	

POLICY STATEMENT

The HECIS seeks to provide its staff, with secure and timely access to the internet and email as necessary for undertaking their work.

The primary purpose for which access to the internet and email is provided by HECIS to its staff is to assist them in carrying out the duties of their employment. Limited personal use may be allowed, but must not impact on performance of duties.

All users of HECIS online facilities and services are expected to be aware of their responsibilities to protect the security of the network, and to use the internet and email accounts in an acceptable manner.

Use of HECIS online services must not jeopardise the fair, safe and productive IT environment of HECIS, nor HECIS operations, assets and reputation.

HECIS online services must not be used unlawfully or for an unlawful purpose.

PROCEDURES

1. Internet and Email Access and Accounts

- All staff are entitled to access to HECIS online services.
- Each staff member is allocated their own HECIS email account.
- Allocation, management and updates of Passwords is managed by the Office Manager.
- HECIS may impose quotas on the use of HECIS online services (including print, file storage, email and internet download) and will revise them as necessary. Where quotas exist, staff are expected to comply with them.
- When staff no longer have a relationship with HECIS or are no longer authorised to have access to HECIS online services, their accounts will be disabled and deleted.
- Staff may have their access suspended immediately where there is a suspected breach of this policy.

2. User Responsibilities

It is a condition of use of HECIS online services that staff do not;

- Use online services to advertise goods or services or for unauthorised commercial activities.
- Use online services for any illegal activity such as sending chain letters requesting money
- **Download software without the approval of the HECIS Co-Ordinator**
- Use online services to access social media sites unless expressly for work purposes
- Create or exchange advertisements, solicitations and other unsolicited or bulk email
- Use online services to access gaming or gambling websites
- Create, send, store, upload, download, access, use, solicit, publish or link to;
    - Offensive, obscene, pornographic or indecent images or material
    - Material likely to cause annoyance, inconvenience or distress to some individuals or cultures.
    - Discriminating or sexually harassing material or messages that create an intimidating or hostile work environment for others.
    - Defamatory material or material that makes misrepresentations or could otherwise be construed as misleading.
    - Material that infringes the intellectual property (including copyright) of another person or organisation e.g. downloading music and videos.
    - Malicious software such as viruses, worms or address-harvesting software.

Users are also responsible for:

- Ensuring individual passwords are secure and not shared with others
- Logging out/turning off of computer systems when they have finished using them.
- Only using HECIS internet and email for purposes relating to their work at HECIS.
- Ensuring printing of online material is kept to minimum
- Ensuring any personal use of HECIS online resources that is granted is kept to a minimum and does not impact on overall productivity.
- Protecting personal information when using online services

3. Organisational Responsibilities and Monitoring of Online Services

- The Office Manager will assist the HECIS Co-Ordinator to manage staff accounts, maintain a secure online environment and keep users informed of their user responsibilities and expected best practice standards.
- HECIS may investigate any and all aspects of its online services if it is suspected that any user of online facilities and services is acting unlawfully or violating this Policy or any other HECIS policy.
- HECIS may monitor, log, collect and analyse the activities of account holders in their usage of online services
- HECIS may filter any network traffic that potentially breaches this policy or is potentially illegal.

4. Consequences of non-compliance

- Any alleged breach of this Policy will be dealt with according to the HECIS Disciplinary Policy.
- Staff breaching this policy may be liable for any loss incurred by HECIS due to inappropriate use by a staff member.

DOCUMENTATION

Documents related to this policy	
Related policies	Disciplinary Policy
Forms, record keeping or other organisational documents	

Reviewing and approving this policy		
Frequency	**Person responsible**	**Approval**
Annually	HECIS Co-Ordinator	Management Committee

Policy review and version tracking			
Review	**Date Approved**	**Signed**	**Next Review Due**
1	26.8.15	HECIS Co-Ordinator	Aug 2016
2	8.8.16	HECIS CoOrdinator	Aug 2017
3	16.8.17	HECIS CoOrdinator	Aug 2018
4	10.9.18	HECIS CoOrdinator	Aug 2019
5	17.9.19	HECIS CoOrdinator	Aug 2020
6	15.9.20	HECIS CoOrdinator	Aug 2021

INDEXING

Search topic/s:	
Function/s:	