

VIEW POLICY ON INTERNET AND EMAIL USE IN SCHOOLS

1. Development of policy

- 1.1 All staff should be consulted when developing email/internet policies. Policies should be constructed from a broad framework that defines acceptable and unacceptable use, defines work related use, gives scope for limited non-work related use, clearly explains the level of monitoring that may be acceptable. Policies should not use definitions that are ambiguous and subjective in interpretation but need to be broad and flexible enough to be workable.
- 1.2 It is not necessary to collect user contracts or signed agreements from staff. Staff do not generally sign other policy documents in schools – Internet/email policies are no exception to this general rule.
- 1.3 Balance between the rights of individuals and the rights of the workplace should be achieved. It is reasonable to have a general principle that email and Internet use should be for work related purposes, but limited non-work related use is also acceptable.
- 1.4 Definitions should be explicit about:
 - Acceptable use
 - Unacceptable use
 - Work related use
 - Non-work related use
 - System or school monitoring

2. Principles for the fair handing of/access to personal information

- 2.1 The following summarises and adapts for the school context National Principles for the Fair Handling of Personal Information (Office of the Privacy Commissioner, 1999). Policies that deal with the issue of monitoring email/internet usage or collecting information for systems should be based on these principles as a starting point.
 - i. Schools/systems should only monitor and collect personal information necessary for legitimate functions or activities
 - ii. Collection of information should be done by lawful and fair means and not in an unreasonably intrusive way
 - iii. Reasonable steps should be taken to ensure that employees are aware of the

- purpose of such information and to whom else such information is disclosed. Employees should have access to this information.
- iv. If the employee has not consented, disclosure of such information to other bodies such as the CEO should only be made if there is a serious breach suspected or serious threat to the organisation.
 - v. In general, schools/systems should take reasonable steps to let employees know the sort of monitoring that may be taking place, for what purpose, and how they collect, hold, use, and disclose that information
- 2.2 If the school has determined to monitor information about individual staff via their emails or internet usage, there should be explicit information provided to staff about the type and purpose of such collection, and which staff members are collecting the information and who has access to this information.
- 2.3 Where an organisation collects information, it will ensure that the subject of this has been made aware of and consented to such collection.
- 2.4 An organisation should not collect information about an employee without their consent and only do so if there is a reasonable suspicion that the employee is breaching school policy.

3. Definitions

This section deals with the need for schools to be explicit and reasonable about definitions of work related internet/email usage

3.1 Work related use

Work related use of email and internet includes (and is not limited to) the following:

- i. Curriculum related information and resources
- ii. Student welfare and pastoral issues
- iii. Professional and educational issues
- iv. Inter-school and external communication with work colleagues
- v. Employment related information – for example, Occupational Health and Safety, union information

3.2 Limited non-work related use

Policies should not prohibit staff from the capacity to send a personal email to a colleague, respond to a query from a friend overseas etc. It is reasonable to require general adherence to work related business, but prohibitive to restrict staff from any personal use.

3.3 Conditions for work and non-work related use

It is more effective to enable work and limited non-work related use of email and the

internet, subject to the following conditions:

- i. Such use is not detrimental to job responsibilities
- ii. Email sent is lawful and does not include defamatory or libelous statements
- iii. Email shall not be used to knowingly distribute pornographic material
- iv. Email shall not be used as a means of sexual harassment
- v. Email shall not be used for sending offensive comments based on an individual's gender, age, sexuality, race, disability, or appearance
- vi. Employees do not knowingly access websites with pornographic materials or those which promote or encourage racism or intolerance

4. Breaches of policy

Breach of the above conditions would constitute unacceptable use. For non-criminal breaches of such protocols, policies may apply temporary measures – for example, discussing appropriate usage, issuing a formal warning or revoking temporarily email use. If a criminal offence is suspected or committed, then the misconduct procedures (CEOM Policy 2.20) should be applied.

Ratified by VIEU Committee of Management and VIEU Councils, 2000