Caerphilly County Borough Council

Directorate of Education & Leisure

Internet: Acceptable Use Policy

Policy on Internet Usage

The council's policy with regarding to access to the Caerphilly County Learning Network is that Internet facilities, both public and in-house, are made available for the use of staff and students where such use will further the strategic aims and objectives of the County Borough. Access to CCLN Internet facilities will be controlled, and use by any individual may be monitored. Any use of the facilities that does not conform to these published guidelines may be considered an offence under the Councils / School's Disciplinary Procedures.

1. Roles and Responsibilities

The following duties apply specifically to Internet use: -

Users must be familiar with and conform to Internet Usage Guidelines.

Head Teachers should publish additional guidelines for the use of Internet facilities by young people. These should include sections on organisation policy, parental permission, teacher supervision and pupil responsibilities.

The Head of IT in conjunction with the Head of Personnel, Head of Legal Services and the Head of Audit will make available all necessary guidance and support to users and will monitor the effectiveness of these guidelines.

2. Access Procedures

Access to Internet facilities will be authorised only via established procedures, which require the user to agree to confirm with the Guidelines, and should be endorsed by the Head teacher.

Access will be provided via the corporate Internet gateway using a Caerphilly County Borough Council standard browser. Users must neither amend the browser configuration, nor make independent arrangements for Internet access.

Some Internet content will be automatically blocked through the use of Internet security features. The fact that some inappropriate content will not be blocked is not authorisation for participants to view that content. If the user finds that they gain access to material of an inappropriate

nature it is their responsibility to ensure that this is reported to the appropriate member of staff, i.e. the system administrator\ICT Co-coordinator who should then report this to the Authority's Education IT department.

3. The primary purpose for the user is to support teaching and learning by providing access to the Internet. Under no circumstances is it acceptable for the user to access the Internet for personal interest purposes.

Internet users must conform to all applicable Personnel Policies and IT Guidelines as well as more specific Internet Usage Guidelines.

4. Unacceptable Use

Certain types of use are not only unacceptable, but may also be illegal. Any user discovered to have intentionally undertaken such use will be liable to disciplinary action.

Examples of unacceptable use include: -

Handling unacceptable material.

It is unacceptable to create, access, copy, store, transmit, or publish material:

- Which is obscene, vulgar, racist, defamatory, or fraudulent;
- Which causes harassment to other;
- Which is likely to irritate or waste the time of others;
- Which is not relevant to the functions of the education institution;
- Which is prejudicial to the Authority's best interests;
- Where such action would breach copyright.

It is unacceptable to undertake any activity that is:

- Intended to access or intercept information in an unauthorised manner (hacking);
- Intended to corrupt any information being held or transmitted on the Internet;
- Intended to detect weakness in the security infrastructure (e.g. testing firewalls, cracking password);
- Intended to disrupt the normal functioning of Internet or related services (e.g. by overloading transactions, introducing viruses).

Downloading of Software

The following rules apply to the downloading of software from the Internet onto one of the school's computers:

- The need and desirability of any proposed download must be properly assessed;
- The computers system administrator must approve any downloading in advance;
- Downloading should only be performed by a technically competent person;
- The computer should have virus protection measures in place;
- The user must accept the risk that downloading may lead to the need for a call for technical support, for which there may be a charge.

5. Internet E-Mail/Mailgear

E-Mail Address (User ID): e-mail messages must be sent and received using only the standard e-mail address format. Individual user ID's will be assigned when the user is given access to the e-mail facility. The sending of anonymous messages is not allowed.

Message Content: all e-mail messages must conform with the guidelines set out in this policy, and in particular must contain no unacceptable material. Messages should be polite and should not contain swear words. Proper attention should be paid to layout, spelling, language, etc, to ensure clarity of the message.

Security and Confidentiality: although the great majority of messages will be delivered successfully to the intended recipients, Internet e-mail must be considered inherently insecure and non-confidential. The following possibilities are likely to occur but should be considered:

- The message may get "lost" in the system;
- The message may be delivered to an unintended recipient;
- The message may be seen by, or even corrupted by, unauthorised users (e.g. hackers).

It would be a sensible precaution for users to ask the recipient of a message to reply with a positive acknowledgement. Additional features are available to enhance the security of e-mail.

6. Control and Monitoring

In order to reduce the risks of users accidentally or deliberately transmitting unacceptable material, the Council will implement the following measures to be applied to groups of users as appropriate:

- Certain Web sites and pages will be made inaccessible;
- Certain words and images will be filtered out if transmitted;
- User activity will be logged and monitoring duties will treat the content of messages as confidential unless unacceptable

material or activity is detected, in which case the incident will be reported to the Education IT Department.

7. Legal Issues

Internet facilities enable the user to handle a very wide range of information. Including personal data, linking to large numbers of computers and other individuals across the world. In this relatively uncontrolled environment, it is particularly important that users are aware and conform to legal requirements. Laws applying to Internet use include: -

- The Computer Misuse Act;
- The Copyright Act;
- The Data Protection Act;

Courts and tribunals treat communication by e-mail exactly as if it were a letter from the Authority or an internal memorandum and legal proceedings can be taken against the Council or an individual in relation to e-mail communications in the same way as action could be taken in relation to letters and memos.

8. Penalties for Improper Use

If it becomes apparent, through monitoring or other means, that an individual has used Internet facilities in a manner that conflicts with these guidelines, then the Authority would invoke their disciplinary procedures. According to the seriousness of the offence, this would result in action that could ultimately lead to dismissal. For certain offences, the individual may also be liable to criminal prosecution under the Computer Misuse Act or the Data Protection Act. You need to be aware that Employment Tribunals have recently upheld dismissals of staff for misuse of Internet access for personal purposes.

I have read and understood the term of this Acceptable Use Policy

Signature	Print Name	Designation