



## **Acceptable Use Policy (AUP) & Procedures**

An Acceptable Use Policy is required to manage access to ICT equipment and Internet access in public libraries. Each authority will have an individual AUP policy reflecting the local circumstances. It is essential to have a written policy and related procedures which are:

- supported by the Legal Department within the Council
- agreed by elected members

It is important that the AUP is reviewed on a regular basis to ensure that it complies with current legislation. The AUP must state that Internet access is monitored using manual and electronic resources and that records of Internet access are kept. These records should be kept for internal and external audit purposes.

The AUP should specify the actions and penalties which could result from contravention of the AUP. This includes providing the police with information where it is suspected that a criminal act has taken place. All library staff should receive appropriate training in the policy and procedures surrounding AUP. A staff training programme and written procedures should be developed to support staff in both ensuring compliance with AUP and the steps which should be taken in cases of contravention.

Specific procedures and penalties should be in place for contravention of the regulations outlined in the AUP and it should be clear that Internet facilities can be withdrawn. Authorities may wish to consider standard letters which will be issued at appropriate stages. The procedures and letters should be agreed with legal sections and supported by elected members.

An example of the framework used for contravention of AUP is:

- a warning letter issued for a first contravention
- a second incident may incur a 6-month ban
- a serious cases, for example illegal activity, would warrant an immediate ban and the incident being referred to the police.

It needs to be clear that where it is suspected that a criminal act has taken place the Council can refer the incident to the police and the Council will provide the police with details of all information accessed.

Policies and procedures need to consider Internet users who are under 16 years of age. In this case the AUP should state that the parent or guardian who signed the AUP or consent form will be notified in the first instance of contravention.



The AUP should explain the practice with regard to filtering and the various levels in place and how users can access appropriate sites which are blocked.

### **Practical Issues Surrounding AUP**

All ICT users must agree to abide by AUP prior to using the Internet and procedures must be put in place to ensure that all users sign up to AUP. Consideration should be given to procedures for children, young people and adults as well as non-members. These procedures should take into account the requirements of Audit Scotland reporting on the number of users of ICT and the number of sessions.

### **Contents of an AUP**

A number of factors have to be included in an AUP including; administration, safety issues, acceptable use and contravention.

### **Administration**

This section should:

- outline who can use the Internet including the procedures for different age groups and parent/guardians giving permission.
- Provide details of the Booking Procedures including how users Log on and off, the maximum length of sessions, how to extend sessions.
- State the maximum number of people at a PC.
- Provide details of any charges.
- State the policy for children using PCs in adult section and adults in children's library.
- Contain a statement about why the library is providing Internet access. This could include the Library Service provides free public access to the Internet in keeping with its role as source of information, intellectual development and enrichment of the community.
- Contain a disclaimer regarding accuracy of content. While the Internet contains valuable and interesting material but some information may be out of date, controversial and offensive or illegal. The authority has no responsibility for quality, accuracy and availability of information.
- Make a disclaimer statement regarding loss, this should be that the Council has no responsibility for any loss, damage or injury as a result of using ICT resources.



### **Safety Issues**

This section of the AUP should:

- Make a statement about security issues and the use of an individuals own equipment or software. This may not normally be permitted but consideration given to exceptions for adaptive technologies. The AUP should state that anti-virus software is installed on all machines, however the Council is not liable for the introduction of viruses to personal equipment following use of Council facilities.
- Contain advice on financial transactions as on-line financial transactions are an increasingly common use of the Internet. You may wish to advise that these should be carried out over secure connections and that the Council cannot be held responsible for any loss resulting from sending confidential information via the Internet.
- Draw attention to personal safety issues. Advice could include the fact that people may not be who they say they are on the Internet and to take care when giving out personal information including address, phone number, email address, school or place of work. Advice should also be that it is wise to leave unsolicited emails unopened and unless users are confident that the source of the email is reliable and that the email will be free from viruses, all unsolicited emails should be deleted without reading.

### **Acceptable Use**

This section should:

- Cover the areas of activity which are prohibited including to accessing, creating or transmitting material that is illegal, offensive, obscene, racist, likely to cause unnecessary offense or distress.
- Include a statement that the librarian will use at their discretion to define material which is considered offensive.
- Draw users attention to Copyright law and should state that users must abide by Copyright law and must not transmit chain letters, spread viruses, or take part in activities including harassment, libel and fraud.
- Encourage users to respect the privacy and confidentiality of others and they must not transmit information, photographs or images of another individual without their knowledge and consent. It should be prohibited to transmit material which is illegal, offensive, obscene, racist or likely to cause unnecessary offence or distress.



### **Contravention**

This section should specify that Internet use is monitored and recorded and that action will be taken in cases where uses are deemed to have misused the service.

This should:

- State the specific procedures and penalties in place for contravention of the regulations outlined in the AUP.
- State that Internet facilities can be withdrawn.
- State the agreed procedures, for example: warning letter may be issued for a first contravention and a second incident may incur a 6-month ban and serious cases may warrant an immediate ban.
- State that where it is suspected that a criminal act has taken place the Council can refer the incident to the police and the Council will provide the police with details of all information accessed.
- State the procedures in place for Internet users who are under 16 years of age.