Managing Safety for Children and Vulnerable Guests in HE

Version: 4

Issued: January 2024

Reference: GEN-DOC-006

Owner: John Chapman

Last Reviewed Date: 21/01/2025

During short visits – for example open days, school visits or summer schools – universities may wish to make their computer systems available to individuals who are regarded by society and the law as unable to take full care of themselves, including children and some adults. While the computers, networks and procedures of school and colleges are routinely designed to cater for these vulnerable users on a permanent basis, universities' systems may not be. (NB the requirements for vulnerable people studying as university students may be different and are not covered here.)

This guide therefore suggests ways that universities and their guests can make such visits safe and successful, by

- developing a separate Acceptable Use Policy (AUP) appropriate for vulnerable users
- providing guidance and training for their own staff supporting these users, and
- agreeing these and any other measures, before each visit, with the school or college and designated adults who are primarily responsible for the users and should know their needs

Acceptable Use Policy

Universities will already have Acceptable Use Policies for their own staff and students. However a different AUP is likely to be needed for vulnerable users, both because visits will generally be short and because of the wider range of unacceptable use, which may include inappropriate content, contact, communication and commerce. This AUP will need to include procedures for identifying and reporting inappropriate activity; users must understand what to do if something goes wrong and how to report incidents or inappropriate content. The AUP must make clear to users what logging and monitoring may be used and by whom. It must be written in appropriate terms so vulnerable users can easily understand it and it must be provided to them before they use the university's systems.

Guidance to Staff

Guidance and training must be provided for staff working with vulnerable users on how to

handle any reports of unacceptable use and on signs that may indicate problems and the appropriate action to take. Staff also need guidance on their own safety. Note that roles that involve contact with children and vulnerable adults may, by law, require Child Protection Training and be subject to Government's Disclosure and Barring Service or the equivalent Scottish scheme.

Responsible Adults

Wherever possible, universities hosting visits from vulnerable users should discuss the arrangements for the visit with those with legal responsibility for safeguarding the users. Schools and Further Education Colleges are normally responsible for safeguarding their pupils during their education, which is likely to include organised visits; parents or guardians are responsible for their children's safety; employers may have some responsibility for those on work placements; and Local Authorities responsible for children in their areas. These discussions should document a clear agreement on the measures that the university will and will not take, and what will be done to resolve any problems. This should include the AUP and Staff Guidance, as well as any additional measures that may be appropriate (see next section). Everyone should be clear that university computers and networks are not the same as systems in either homes or schools and they should know what steps will be in place to safeguard learners using them.

Additional Measures

Depending on the type of visit and users involved, a variety of further measures may be appropriate. Some examples are given here. Many of these are likely to involve the host university in additional effort or changes to their systems so may not always be possible. Additional measures should be agreed as part of the prior discussions, especially if any are considered essential for the visit to take place as planned.

- As well as providing users with the Acceptable Use Policy, a clear notice reminding them of safe behaviour/e-safety rules may be helpful.
- Additional monitoring of use of computers and the Internet may be appropriate, for example direct supervision by accompanying adults or online monitoring and logging of the activity of individual users. Note that this may involve new privacy and safeguarding issues: for example moderators of children's chatrooms may be subject to the Disclosure and Barring Service. All users must be told what monitoring and logging is used.
- Separate physical (and possibly network) space may be considered for the visit to avoid conflicts with other users.
- Users may be limited to using designated physical terminals and/or accounts that have been checked for safety and have restricted permissions and access. If they can connect their own devices to university wired or wireless networks then safety will be much harder to manage.
- Content or protocol filtering may be possible on either PCs or networks, though this will have to be configured to meet the particular policy requirements of each group of visitors.
- Enabling a user to suspend internet access and report a problem immediately (a 'Stop Now' button) may help in dealing with inappropriate use.

Resources

SWGfL’s online safety policy templates [1]

Click CEOP Safety Centre [2]

Links
[1] https://swgfl.org.uk/resources/online-safety-policy-templates
[2] https://www.ceop.police.uk/safety-centre/