Ensuring adequate safeguards for children and young people while using allocated computer equipment

Introduction

This guidance covers all computer equipment[1] assigned to children and young people that is, or may be, used away from council premises. It applies to all equipment supplied through any official procedure or scheme, regardless of the source of funding. It does not apply to equipment purchased privately by family members.

Professionals working with and for children and young people have a duty of care to provide sufficient safeguards to protect them while using designated computers and the internet, wherever that use takes place. **This document is concerned only with the technical actions needed to ensure safer access through such equipment, not aspects of encouraging safer behaviour and responsible use through education.**

Although the bulk of this guidance relates to use of the internet, the principles apply equally to using equipment while offline. The guidance includes a checklist to identify any issues or gaps in service provision.

Use of computer equipment while on Council premises

Schools, youth centres and other Council-run or controlled premises used by children and young people already meet government standards for managing internet access through the adoption of the London Grid for Learning[2] (LGfL) as internet service provider (ISP). This is guidance is intended to be suitable safeguarding protection in the vast majority of cases, but you may wish to review any technical settings at appropriate time periods.

In some circumstances the standard web filtering profile may require modification to suit the needs of a particular child. LGfL offers individualised user-level filtering to address this need.

Some establishments implement additional levels of safeguarding through the use of proactive systems (such as Securus[3]) that monitor use for patterns symptomatic of risky or other behaviour, such as bullying and self-harm. Access to such technology may be particularly useful for professionals working with vulnerable children and young people on council premises.

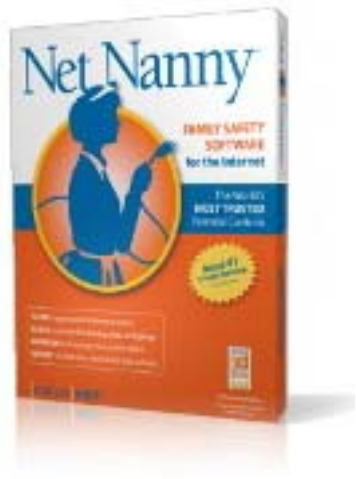
---

[1] "Computer equipment" encompasses all items capable of connecting to the internet, such as laptops but including most mobile phones, tablet computers (including iPads), plus hand-held and standard gaming consoles.
[2] LGfL safeguarding policies: http://www.lgfl.net/information/about/Pages/Policies.aspx
[3] http://www.securus-software.com

Use of computer equipment while off council premises

Some children and young people have equipment allocated to them for use while away from Council premises. Since such use is likely to be in less regulated circumstances, it is particularly important that adequate safeguarding protection is installed on the equipment prior to its first use. As a minimum, the chosen safeguarding solution must prevent access to pornography, other 'adult' content and extreme material such as racist sites.

Laptops and netbooks



In the case of laptops, this is most easily achieved through installation of a safeguarding product such as Net Nanny[4].

Net Nanny and its competitors are subscription services. It is therefore important to maintain the account subscription, so that the protection remains up to date. This must be factored in to the total cost of ownership.

Products such as Net Nanny also allow access to be managed by time of day or amount of use – for example, 60 minutes of Facebook per day and no use after 9pm.

Many also offer a level of proactive protection, such as monitoring social networking conversations for grooming or bullying behaviour, and can alert a responsible adult should such activity be detected.

It is essential that the administrator password for the chosen product is not available to the child or young person, since that would allow protection to be switched off.

Other equipment

For non-laptop equipment, the main risk to satisfactory safeguarding is unfiltered access to the internet through 3G/4G and WiFi access. This is a particular issue since products such as the above are generally not available for mobile equipment and games consoles, and even if they are, may be relatively easy to bypass.

While the actual methods to minimise risk will vary depending on the equipment, the general principles are:

- Where access to the internet is available through a 3G/4G contract with a telephony company, the company must supply filtered access appropriate to the age of the end user (child or young person).
- WiFi access must either be disabled or restricted to approved networks that offer the same degree of age appropriate pre-filtering.

Consult your technical support staff to help you to achieve these outcomes.

---

[4] http://www.netnanny.com/products/netnanny

Safeguarding children and young people with allocated computer equipment

Checklist of good practice

Laptops and netbooks

- There is a maintained inventory of all computer equipment allocated to children and young people ☐
- All equipment is equipped with appropriate safeguarding software ☐
- The safeguarding software is kept up to date ☐
- The end user has no access to any administrator account password(s) ☐

Mobile phones

- There is a maintained inventory of all mobile phones allocated to children and young people ☐
- 3G/4G internet access is filtered at an age appropriate level ☐
- WiFi access is either disabled or locked down to known approved services ☐
- The end user has no access to any administrator account password(s) ☐

Games consoles (including hand-held)

- There is a maintained inventory of all games consoles allocated to children and young people ☐
- WiFi access is either disabled or locked down to known approved services ☐
- Parental controls are enabled and set to an age appropriate level ☐
- The end user has no access to any administrator account password(s) ☐

For further help, please contact the ICT and E-safety Adviser:
Peter Cowley
p.cowley@richmond.gov.uk
020 8831 6225
07595 173975