The Association of National Specialist Colleges

Natspec www.natspec.org.uk

Natspec e-safety policy framework: draft

Background

This paper outlines the key elements of a policy framework for ensuring the safety and security of learners with LDD in ISCs and other settings, who use technology of all kinds for learning, leisure and independence. The paper arises from discussions at the Natspec/TechDis e-safety working group meeting. At this stage, we would welcome:

- general feedback
- specific comments, in particular on any issues that have been omitted
- offers of case studies to illustrate aspects of this work, including examples of where things have gone wrong and creative approaches that have worked

It is our intention to issue this as guidance that will help colleges to develop their own policy, customised to their particular setting and to their learners' needs. The more confident that colleges become in being open about these issues, the better they will be able to support their learners in the use of a wide range of technology, including their own mobile technology.

Purpose of a policy

We suggest that the purpose of an e-safety policy would be:

- To ensure that learners with LDD continue to benefit from technology, used for whatever purpose, and are able to do so safely and responsibly, and with confidence

- To ensure that staff throughout the college have the confidence to provide an appropriate level of support to learners in the safe and responsible use of technology

- To enable colleges to develop guidance and practice that reflects and is in keeping with their ethos and that builds on and links into existing policies, such as IT and risk assessments

The aim is to produce a clear framework, including legal aspects, for work in this area, that promotes a positive and constructive approach rather than

focussing on the risks. It is an area in which it can be tempting to take a negative approach based on restricting use and access and telling learners and staff what they can't do, rather than teaching them how to do it safely. There are understandable reasons for this:

- Staff are anxious about what is and is not appropriate for learners, and will have differing views
- Technology changes and develops quickly – and sometimes learners embrace these changes more readily than staff
- Building flexibility into IT systems is essential if you want to promote wider access and use, but more challenging if it is managed off site.
- The legal framework is complex and encourages college managers to err on the side of caution
- The views and expectations of parents will vary considerably

The framework proposes that an e-safety policy must be driven by the needs of users, both learners and staff, rather than by the technology – it should make sense to the IT phobic as well as the IT department. It should help colleges to prepare learners to cope with the IT challenges of the real world. We propose to develop a simple audit/checklist to sit alongside the policy.

The context

We propose two main strands to the framework. One of these will reflect specific issues linked to the residential setting; in most GFEs, issues around e-safety and filtering are more readily managed because they are exclusively educational settings. In a residential setting, which becomes a student's home, there may need to be a different approach to this issue, equally vigilant but more relaxed. The second strand will reflect the specific needs of those with learning difficulties and/or disabilities, so that ISCs can be proactive in developing a curriculum that teaches learners to use technology safely and securely.

We are aware that other providers will be interested in this work; for example, it has application in other residential settings such as agricultural colleges and care homes, and in LLDD departments in GFEs.

The college ethos

All policies will reflect the individual college ethos, as outlined in the mission statement and values. Many ISCs promote adult status, listening to learners, maximising independence and work related activities; a restrictive approach to the use of technology cannot be in keeping with such goals, especially when technology has been so liberating for many learners. At the same time, it is essential to afford a level of protection for vulnerable learners who may have difficulty making sound or consistent judgements about some of the opportunities offered through technology.

Possible elements for inclusion in policy

We suggest that the following considerations will inform the policy:

- Appropriateness
- Legality

- Safety
- Security
- Risk (to individuals and the college)
- Opportunity

These aspects will differ in relation to individual learners and in relation to the setting (teaching or residential).

A comprehensive policy could include the following areas:

1. Using technology within the law, including copyright, data protection and legal/illegal activities such as terrorist/paedophile related sites
2. Using email
3. Using texts and instant messaging
4. Access to 'adult' sites, including pornography and gambling
5. Social networking
6. Mobile technology
7. Buying on the internet
8. Using search engines
9. Creating websites
10. Blogging
11. Working with parents

Colleges may wish to develop an e-safety profile for each learner as part of their risk assessment; this should consider the risk of that learner being a perpetrator as well as a victim of technology related abuse. This might also indicate the extent to which this learner will be able to learn from mistakes in an ICT context.

Most learners will need learning goals relating to e-safety within their learning programme.

The curriculum

We hope to develop resources to support a curriculum that covers all the areas outlined above. There are many resources with good content available already, but these tend to be wordy, over-crowded with information and not targeted at an LLDD audience.

The most useful approach would be to develop a set of simulation activities with built in warning systems, such as a red light or siren, if a learner was about to put personal information on a social networking site or did not check for the 'secure site' logo when purchasing goods. Ultimately, this could be developed as a live system.

Staff training

It will be essential to underpin this with on-going staff training, included as part of regular safeguarding training. It will aim to ensure that staff have a consistent approach to all areas of the policy and feel confident about implementing it around the college.

Natspec/TechDis e-safety working group, May 09