Leven CE (VC) Primary School

ESAFETY & INTERNET USE

November 2014

1. Why is Internet use important?

The internet has become increasingly accessible for children and young people in places like schools, libraries and their own homes. Children and young people will experiment online, to enable them to take advantage of the many educational and social benefits of new technologies learners need opportunities to create, collaborate and explore in the digital world, using multiple devices from multiple locations. However, all users need to be aware of the range of risks associated with the use of these internet technologies alongside the development of safe and responsible online behaviours.

Possible Statements:
- The Internet is a part of everyday life for education, business and social interaction. The (name of organisation) has a duty to provide children and young people with Internet access.
- Children and young people use the Internet widely outside school and need to learn how to evaluate Internet information and to take care of their own safety and security.
- Internet use is part of the statutory curriculum and a necessary tool for learning.
- Internet access is an entitlement for students/children and young people who show a responsible and mature approach to its use.
- The purpose of Internet use in (name of organisation) is to raise educational standards, to promote pupil/children and young people's achievement, to support the professional work of staff and to enhance the (name of organisation) management functions.

2. How does Internet use benefit children and young people?

A number of studies and government projects have identified the benefits to be gained through the appropriate use of the Internet.
Benefits of using the Internet include:

Possible statements:
- vocational, social and leisure use in libraries, clubs and at home;
- access to experts in many fields for pupils and staff;
- educational and cultural exchanges between pupils world-wide;
- access to world-wide educational resources including museums and art galleries;
- professional development for staff through access to national developments, educational materials and effective curriculum practice;
- collaboration across networks of schools, support services and professional associations;
- exchange of curriculum and administration data with HCC and DfE;
- access to learning wherever and whenever convenient.

3. How can we ensure Internet use enhances learning and life experiences?

Children and young people need to learn digital literacy skills and to refine their own publishing and communications with others via the Internet. Respect for copyright and intellectual property rights, and the correct use of published material should be taught.

- The school Internet access will be designed to enhance and extend education.
- Children and young people will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- The school will ensure that the copying and subsequent use of Internet derived materials by staff, children and young people complies with copyright law.
- Access levels will be reviewed to reflect the curriculum requirements and age of children and young people.
- Staff should guide children and young people to on-line activities that will support the learning outcomes planned for their age and maturity.
- Children and young people will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- Children and young people will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

4. How will children and young people learn how to evaluate content?

Information received via the Internet, email or text message requires good information handling and digital literacy skills. In particular it may be difficult to determine origin, intent and accuracy, as the contextual clues may be missing or difficult to read.

The extent to which the internet is used by extremists as a tool for radicalisation is not fully known , but it is clear that that persons responsible for recent attacks have accessed and been influenced by the internet to varying degrees.
Extremist websites may be used to disseminate propaganda, spread news and updates on extremist issues, add radical interpretation to theological tracts and provision of discussion forums for like minded individuals.
The internet also offers easily accessible downloadable extremist material including advice and guidance on bomb making, filtered out of public systems, but often not at home – policies need to empower children and young people to evaluate content critically.

Possible statements:

- Children and young people should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- The evaluation of on-line materials is a part of teaching/learning in every subject.

5. Prevent Strategy

The current threat from Terrorism and Extremism in the United Kingdom is real and severe and can involve the exploitation of vulnerable people, including children and young people.

With this information, we hope to provide a clear framework to structure and inform our repsonse to safeguarding concerns for those young people who may be vulnerable to the messages of extremism. In addition, it provides details of the local inter agency process and expectations in identifying appropriate interventions based on the threshold of need and intervention model and the Channel process. (See below)

Radicalisation is defined as the process by which people come to support terrorism and extremism and, in some cases, to then participate in terrorist groups.

Extremism is vocal or active opposition to fundamental British values, including democracy, the rule of law, individual liberty and mutual respect and tolerance of different faiths and beliefs. We also include in our definition of extremism calls for the death of members of our armed forces, whether in this country or overseas (HM Government Prevent Strategy 2011).

1. Equality, Diversity and Community Cohesion

The school aims to teach pupils to understand others, to promote common values and to value diversity, to promote awareness of human rights and of the responsibility to uphold and defend them, and to develop the skills of participation and responsible action. We take extremely seriously our key role in preparing all our young people for life in modern Britain.

We aim to encourage working towards a society in with a common vision and sense of belonging by all. Communities; a society in which the diversity of people's backgrounds and circumstances is appreciated and valued; a society in which similar life opportunities are available to all; and a society in which strong and positive relationships exist and continue to be developed in the workplace, in schools and in the wider community

1. National Guidance and Strategies

PREVENT is a key part of the Government's strategy to stop people becoming terrorists or supporting terrorism. Early intervention is at the heart of PREVENT in diverting people away from being drawn into terrorist activity. PREVENT happens before any criminal activity takes place. It is about recognising, supporting and protecting people who might be susceptible to radicalisation. The PREVENT strategy objectives are:

<u>Ideology:</u> respond to the ideological challenge of terrorism and the threat we face from those who promote it.
<u>Individuals:</u> prevent people from being drawn into terrorism and ensure that they are given appropriate advice and support
<u>Institutions:</u> work with sectors and institutions where there are risks of radicalisation which we need to address.

Partnership Working

Awareness of PREVENT and an understanding of the risks it is intended to address are both vital. Professionals can help to identify, and to refer to the relevant agencies, young people whose behaviour suggests that they are being drawn into terrorism or extremism. Schools can help to protect children from extremist and violent views in the same ways that they help to safeguard children from drugs, gang violence or alcohol. School's work on PREVENT needs to be seen in this context. The purpose must be to protect young people from harm and to ensure that they are taught in a way that is consistent with the law and our values.

All organisations should have an awareness of the PREVENT agenda and the various forms of radicalisation takes in being able to recognise signs and indicators or concern and respond appropriately.

5. How will information systems security be maintained?

It is important to review the security of the whole system from user to Internet. This is a major responsibility that includes not only the delivery of essential learning services but also the personal safety of staff, children and young people.
Data security is a complex matter and cannot be dealt with fully in this document. However, the person in charge of data security needs to be identified within the organisation; this could be a network manager, business manager, or technical manager. Note the role is distinct and separate from the 'E-safety co-ordinator', a role identified in 3.2.1.
All staff with access to personal data are liable in law to protect that data. Should data be lost from an unencrypted USB drive or seen on a laptop used by other people, the consequences could be serious for the member of staff, for the school or organisation.
Local Area Network (LAN) security issues include:

Possible statements:
- Access to all ICT systems shall be via unique login and password. Any exceptions shall be recorded in the risk assessment and approved by the person in charge of data security.
- Where possible, all information storage shall be restricted to only necessary users. Access granted to new groups of users (for example, an external group attending a school-based event) shall be approved by the person in charge of data security.
- All requests for access beyond that normally allocated (e.g. teachers wishing to access pupil personal storage) shall be authorised by the person in charge of data security. This shall include the authorisation of access required by the ICT Support Team during investigations.
- Where 'restricted' information is stored, access shall only be granted to individuals approved by the person in charge of data security. A record shall be kept of these approvals.
- All access controls should be reviewed each term, to ensure that any users that leave have their access removed.
- Users must act reasonably — e.g. the downloading of large files during the working day will affect the service that others receive.
- Users must take responsibility for their network use.

• Workstations should be secured against user mistakes that compromise access or security and deliberate actions.
• Servers must be located securely and physical access restricted.
• The server operating system must be secured and kept up to date.
• Virus protection for the whole network must be installed and current.
• Access by wireless devices must be pro-actively managed and must be password protected.
• Portable media may not be used without specific permission followed by a virus check.
• Unapproved software will not be allowed in pupils'/staff work areas or attached to email.
• Files held on the organisation's network will be regularly checked.
• The person in charge of network management will review system capacity regularly.

6. How will filtering be managed?

Levels of Internet access and supervision will vary according to the child or young person's age and experience. Access profiles must be appropriate for all members of the organisation.

• Leven CE (VC) Primary School will use the LA mediated filtering systems to ensure that systems to protect children and young people are reviewed and improved.
• Requests for filtering changes from within the organisation will be made via the Headteacher.

Organisations installing their own filtering systems are taking on a great deal of responsibility and demand on management time. Hundreds of inappropriate sites are created each day and many change URLs to confuse filtering systems.

Possible statements:
• The organisation's broadband access will include filtering appropriate to the age and maturity of children and young people.
• A senior member of staff in the organisation will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
• Any material that the organisation believes is illegal must be reported to the appropriate agencies such as Children's Social Care, IWF or CEOP.
• The organisation's access strategy will be designed to suit the age and requirements of the children and young people, with advice from network managers.

7. How will videoconferencing be managed?

Videoconferencing enables users to see and hear each other between different locations. This 'real time' interactive technology has many uses in educational settings.
The National Educational Network (NEN) is a private broadband, IP network interconnecting the ten regional schools' networks across England with the Welsh, Scottish and the Northern Ireland networks.

Schools with full broadband are connected through the YHGfL and have access to services such as gatekeepers and gateways to enable schools to communicate with external locations.

Conferences should always be booked as private and not made public. The conference URL should only be given to those who you wish to take part.

The equipment and network
• All videoconferencing equipment must be switched off when not in use and not set to auto answer.
• Equipment connected to the educational broadband network should use the national E.164 numbering system and display their H.323 ID name.
• External IP addresses should not be made available to other sites.
• Videoconferencing contact information should not be put on the school Website.
• The equipment must be secure and if necessary locked away when not in use.
• Videoconferencing equipment should not be taken off (name of organisation) premises without permission.

Users
• Videoconferencing should be supervised appropriately for the young person's age.
• Parents and carers should agree for their children to take part in videoconferences, probably in the annual return.
• Only key administrators should be given access to videoconferencing administration areas or remote control pages.
• Unique log on and password details for the videoconferencing services should only be issued to members of staff and kept secure.

Content
• When recording a videoconference lesson, written permission should be given by all sites and participants. The reason for the recording must be given and the recording of videoconference should be clear to all parties at the start of the conference. Recorded material shall be stored securely.
• If third-party materials are to be included, check that recording is acceptable to avoid infringing the third party intellectual property rights.

8. How can emerging technologies be managed?

Many emerging communications technologies offer the potential to develop new teaching and learning tools, including mobile communications, collaboration and multimedia tools.
A risk assessment needs to be undertaken on each new technology for effective and safe practice in classroom and/or organisational use. The safest approach is to deny access until a risk assessment has been completed and safety established.
Virtual online classrooms and communities widen the geographical boundaries of learning. The safety and effectiveness of virtual communities depends on users being trusted and identifiable.
There are dangers for employees/volunteers however if personal phones are used to contact children and young people and therefore an organisationally owned phone should be issued.
Abusive messages should be dealt with under the organisation's behaviour and/or anti-bullying policies.

Possible statements:

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in the organisation is allowed.
- Staff will be issued with an organisation phone where contact with children and young people is required.
- The sending of abusive or inappropriate text, picture or video messages is forbidden.

9. How should personal data be protected?

The quantity and variety of data held on children and young people, families and on staff is expanding quickly. While this data can be very useful in improving services, data could be mishandled, stolen or misused.

The Data Protection Act 1998 gives individuals the right to know what information is held about them and provides a framework to ensure that personal information is handled properly. It promotes openness in the use of personal information. Under the Act every organisation that processes personal information (personal data) must notify the Information Commissioner Office, unless they are exempt.

The Data Protection Act 1998 applies to anyone who handles or has access to information concerning individuals. Everyone in the workplace has a legal duty to protect the privacy of information relating to individuals.

The Act sets standards (eight data protection principles), which must be satisfied when processing personal data (information that will identify a living individual). The Act also gives rights to the people the information is about i.e. subject access rights lets individuals find out what information is held about them.

The eight principles are that personal data must be:

- Processed fairly and lawfully;
- Processed for specified purposes;
- Adequate, relevant and not excessive;
- Accurate and up-to-date;
- Held no longer than is necessary;
- Processed in line with individual’s rights;
- Kept secure;
- Transferred only to other countries with suitable security measures.

Organisations will already have information about their obligations under the Act, and this section is a reminder that all data from which people can be identified is protected.

10. Password security

Members of staff/volunteers with access to ICT systems shall be responsible for taking the appropriate steps to select and secure their passwords.
These steps should include:

- Keeping their password secure from others.

- Using a different password for accessing organisational systems to that used for personal (non-organisational) purposes.
- Choosing a password that is difficult to guess, or difficult for others to obtain by watching them login.
- Adding numbers or special characters (e.g. !@£$%^) can help.
- Changing passwords regularly e.g. every three months.
- Staff/volunteers should try not to write down their password, unless absolutely necessary and then in a location that cannot be accessed by anyone else.
- In addition, when leaving a computer for any length of time, all staff members/volunteers shall log off or lock the computer, using CTRL+ATL+DELETE or other system command.