Bath and North East Somerset
Local Safeguarding Children Board

LSCB - E-safety Strategy

Introduction

The rapid growth of the internet and of electronic technologies has opened up a world of exciting opportunities for many children and young people. Through the internet and mobile technology it is possible for young people to have access to almost unlimited information worldwide, to be entertained with films and music and, through social networking sites to contact and socialise with other young people. However alongside the benefits there are also risks, and while most young people are very competent in using these technologies, their knowledge and understanding of the risks is often very low.

The risks to children and young people are various: being exposed to inappropriate content; being groomed by someone who wants to abuse them; being bullied on line or via mobile technology; blackmailed; of having their identity stolen; and of being the subject of fraud. Children and young people need to be protected from these risks and they need to be helped to develop the skills to keep themselves safe when they are on line.

The Children Act 2004 and the Every Child Matters programme established the 5 Outcomes - that children and young people should be safe and healthy, should enjoy and achieve in their lives and be able to make a positive contribution and achieve economic wellbeing .The Local Safeguarding Children Board has a key role to play in promoting the welfare of children and young people and in particular in ensuring that they are safe. It is recognised by Bath and North East Somerset LSCB that ensuring children and young people are safe when they are on line is a key part of that responsibility to help children stay safe.

This strategy has been written to provide the E-Safety framework for member agencies of the LSCB and other agencies and organisations who work with children in order that the children and young people of BANES can be safe when they are on line or using ICT technologies. The strategy recognises that being safe online is not just a matter of technology but that a comprehensive approach to e-safety is necessary, in which children and young people are kept safe by sound policies that inform technical standards , alongside a programme of education for them and their carers which develops and sustains safe on line behaviour. The strategy will be monitored by the LSCB to ensure that it remains relevant to its objectives and so that it can develop as the information technologies change and evolve.

E-Safety Strategy

The aim of the E-Safety Strategy is to provide all children and young people in Bath and North East Somerset with a safe electronic environment where they can learn, explore, socialise and enjoy themselves.

The strategy was approved by the Local Safeguarding Children Board on 2nd December 2008.

The implementation of the policy will be monitored by the E-Safety Working Group who will report to the LSCB.

Monitoring of the implementation will take place each month for the first year and then at intervals agreed by the LSCB.

The strategy will be reviewed by the LSCB annually who will receive annual report from the E-Safety Working Group after the first year and subsequently the E-Safety Co-ordinator.

The strategy action plan for E-Safety in Bath and North East Somerset is arranged in the following main areas -

Policies

All of the E-Safety strategy needs to have a foundation of agreed policies that direct agencies, professionals, parents and young people in the safe use of the internet.

These policies must include:

- Acceptable use policies
- Internet filtering policies
- Procedure for reporting incidents including an incident flow chart

These will need to be interpreted into E-Safety policies that can be applied to schools and other agencies.

Infrastructure

Access to the internet needs to be through equipment and connections that will allow for a good level of protection, filtering, and professional/parental control. This strategy will establish what the standard should be and how agencies and individual families can enable this.

Education

Technical measures alone will not keep children and young people safe .There will need to be a comprehensive education and training for professionals, parents and young people to learn about the risks of the internet and about the behaviours that are needed to stay safe online. This will be centred on schools in the main, but not exclusively, and will provide training/information sessions to teachers and other professionals, parents and to children and young people.

Supervision /Monitoring

Once measures are put in place it will be necessary to monitor their effectiveness and be prepared to alter and update them as changes emerge in the internet. This will happen via the E-Safety Working Group initially.

Organisation and Accountability

Each agency that forms part of the LSCB has appointed an E-Safety Officer. This group of appointed agency E-Safety Officers will have the day to day responsibility for the direction and implementation of the B&NES strategy for their agency. Each E-Safety Officer will need to signpost and advise staff in their agency on e-safety issues, identify training needs and ensure that incidents are dealt with according to the incident flow chart, and provide annual returns regarding all incidents, including bullying, to the E-Safety Co-ordinator.

Each school and service or agency that works directly with children and young people will need to identify an E-Safety Officer who will have the responsibility for promoting and co-ordinating the E-Safety Policy for that part of the agency. These E-Safety Officers will be required to carry out the same functions as set out for LSCB member agencies, as set out above.

B&NES LSCB Actions: Policies

Policies provide clear guidance for safeguarding and promoting the welfare of children and young people in an ICT environment. Such policies should address training and computer hardware requirements, and also internet access for key staff.

All LSCB agencies will need to consider the E-safety issue within their organisation and how the various elements i.e. acceptable use policies; use of mobile technologies etc will impact upon their staff and business operations

The policies to guide safety will include -

Acceptable Use Policies

Acceptable use policies promote responsible use of the internet by ensuring that users are responsible and safe, that they are not exposed to any damaging material and that systems are protected from accidental or deliberate misuse .They will apply to professional staff, volunteers and children and young people.

Agencies should;

- Periodically review and update their AUP in line with the revised B&NES Internet Policy
- Ensure that every user (Children, young people & parent where applicable) has read and signed the AUP to say they accept the policy
- Ensure educators, leaders, carers and users are aware of how to report incidents
- Provide advice and guidance to parents on how to protect their child at home.

Develop model policies (using best practice examples)

The South West Grid for Learning (SWGfL) has produced a school e safety policy which provides schools with the templates and infrastructure that they will need to have a comprehensive E-Safety policy. It can be adapted and modified as appropriate for each school. The school E-Safety Policy has been adapted as a template to be used by LSCB and other agencies.

Schools Internet Policy document

The Schools Internet Policy document produced by B&NES Children's Services is regularly revised and updated. The current version should be reviewed to include new and emerging technologies. The revised version should include clear advice to schools, with an expectation to state their response actions to ICT abuse e.g. discipline procedures and prevention methods.

Child Protection Policy

The child protection policy will address any incidents of misuse that are also abusive. They will include:

- Child sexual abuse images
- Adult material which potentially breaches the Obscene publications act
- Criminally racist material
- Other criminal conduct, activity or materials

This policy will be a part of the child protection procedures and any incident that is considered to be abusive will be investigated according to the child protection and/or allegations management procedures.

Infrastructure Produce a register of Internet access locations

Through an audit, produce a register of locations where B&NES either directly or indirectly provide Internet access which can be used by children and Young People, (excluding schools).

Security software

All agencies in the B&NES area need to review the security software currently available on its sites and install suitable security to reduce the risk of virus, Trojans, adware and cookies. Establishments may require specialist advice from B&NES E-Safety working group.

A review of what filtering products (if any) other establishments including, Youth Centres, Libraries, Further Education and Health within B&NES currently have will need to be undertaken.

Age related filtering and blocking

Agencies and organisations will need to establish their own filtering and blocking criteria that meets the minimum requirements set out by the LSCB. Standard default settings will be advised but each establishment must determine which sites they will block and which sites will be allowed to be viewed by certain age groups.

Evaluate how schools and other establishments currently operate their local filtering

The E-Safety Working Group will continue to research current practice, analyse statistical evidence from the SWGfL filtering and where requested, provide information and costing for those establishments without appropriate filtering.

Spam filtering and blocking

Ensure that every school uses effective filtering / blocking systems. Where schools use the SWGfL network, they are provided with a sophisticated filtering product. The product is controlled centrally for primary schools however secondary schools should ensure that educators as well as technical support staff fully understand how it works so they can apply local policies.

Education

The education of children and young people, their parents and carers and the professionals that support them is an essential part of the E-Safety Strategy .As stated above e-safety is not just a technological issue and the education of children and young people in developing the behaviours that will keep them safe when they are online, is a key preventive measure.

There will be a comprehensive education programme which will be available to all who need this to establish the basic principles of e-safety. In addition there will be specific training to particular groups of children and young people in a rolling programme.

The 3 initial areas for delivery to parents, children and young people in Phase 1 are

1. Schools
2. Youth Service
3. Children in Care

Additionally, phase 2 will consider:

1. Libraries
2. Children Centres
3. Health Clinics/Visitors
4. Voluntary Organisations

Children and young people

The majority of children and young people will be educated about issues of e-safety through their schools. The education they will receive will be part of their general education in order that the habits of good practice will become part of their behaviour when they are using the internet at school and will therefore promote safe behaviour when out of school.

Parents and carers

There will be a number of parent information evenings provided by the LSCB, **in addition** to sessions that schools may arrange themselves, that will be available to all parents to inform them about e-safety and provide straightforward, accessible guides .This will be followed up by written information for reference.

Professionals

There will be specific training for E-Safety Officers and teachers in order that they will be able to promote the e safety programme to their students and parents.

Information sessions for foster carers and professionals working with children and young people will also be provided via the LSCB Inter-agency Safeguarding training programme and/or SWGfL.

In addition to this programme there will be the following actions -

Consultation with children and young people

Children should be made aware of the issues of e-safety through PSHE and other means, and should be provided with opportunities to express their views and concerns. Agencies need to consider opportunities to involve and consult with children and young people through the development of e-safety policies, school events, Youth Centres, Stakeholder events and Youth Groups i.e. DAFBY.

Promotion of the new Child Exploitation and Online Protection Centre

A national campaign is in place to provide an easy and accessible means of reporting incidents and concerns. B&NES LSCB supports this campaign and will seek to ensure that all B&NES' child accessible computer desktop screens display a shortcut to the 'Think U Know' site.

Extended schools and community development

Consideration should be given to the development of volunteer schemes to match the expertise of industry to the needs of parents and communities as part of the extended schools agenda, especially as learning may take place under the supervision of external organisations.

Monitoring and auditing implementation

On an annual basis, E-Safety Officers will be required to undertake an audit of their e-safety policies etc. and provide returns on incidents to the E-Safety Co-ordinator. The LSCB will receive a collated audit report from all agencies.

January 2009