eSafety

E-SAFETY POLICY GUIDANCE
JUNE 2011

1 Introduction

1.1 The guidance presented in this document is intended to help agencies that deliver services to children and young people to develop an **e-Safety Policy**. It covers key areas that the policy should include and is designed to be used in conjunction with the **BMBC Information Security and Computer Usage Policy** and your **eBehaviour Agreements**.

1.2 It is the responsibility of the agency to read and apply this guidance to the development of an appropriate eSafety policy that meets the needs of and is appropriate to each individual setting.

2 Background

2.1 New technologies have become integral to the lives of children and young people in today's society, both within and out of their school lives. It forms a key part of both their learning and their social lives, particularly since the developments in mobile technologies such as Smart Phones.

2.2 The internet and other digital information technologies are powerful tools, which open up new opportunities for everyone. In its early days the internet was simply a mechanism where people could place material for others to read and download, however the recent developments in the internet technology, the drive is towards creation communicate and contribute. This has led to the growth of what is now referred to as Web 2.0 where 'social networking' and 'collaborative environments' are common place, no longer do young people sit and look they contribute, develop and share. Electronic communication helps adults and young people learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe internet access at all times.

2.3 The requirement to ensure that children and young people are able to use the internet and related communication technologies appropriately and safely is addressed as part of the wider duty of care to which all who work with them are bound. A school **e-Safety Policy** should help to ensure safe and appropriate use. The development and implementation of such a policy should involve all stakeholders in a child or young person's life, whether at school, home, out in the community or in care.

2.4 The use of these new technologies can put young people at risk, some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to, loss of, sharing of personal information
- Risk of being subject to grooming by those with whom they make contact
- The sharing and distribution of personal images without their consent
- Inappropriate communication and contact with others
- Cyber-bullying
- Access to unsuitable video and internet games
- An inability to evaluate the quality, accuracy and relevance of e-information
- Plagiarism and copyright infringement
- Illegal downloading of music and video files
- Excessive use impacting on social and emotional development

2.5 The agency that delivers services to children and young people must demonstrate that it has provided the necessary safeguards to help ensure that they have done everything they can reasonably be expected to do in order to manage and reduce these risks. The guidelines that follow should assist the agency to develop a policy that explains how they do this, while addressing wider issues, in order to

help young people (and their parents / carers) to be responsible users and stay safe while using the internet and other communications technologies.

3 What details should an eSafety policy include?

3.1 An eSafety policy should include detail around the following areas:

- Scope of the Policy
- Roles and Responsibilities
- Policy Statements (relative to the individuals and context of the policy)
- Incident Management process in the event of an eSafety incident
- Reference to eBehaviour Agreements
- Reference to the Information Security and Computer Usage Policy (BMBC)

4 Scope of the Policy

4.1 This should include general statement about the scope of the policy, the establishment which it covers, and the members of the establishment that are to be bound by the policy.

5 Roles and Responsibilities

5.1 Under this section it is important to highlight the individuals to whom the policy applies, within the establishment, and what is expected of them. An example statement would be *'the Governors are responsible for the approval of the e-Safety policy and for reviewing its effectiveness. This will be carried out through [process]. A member of the Governing Body [name if applicable] has taken on the role of e-Safety Governor. The role of the e-Safety Governor will include…….'.*

5.2 It is important to highlight each group of individuals and state clearly what is expected of them in relation to e-Safety. Example groups include:

- Governors
- Headteachers
- E-Safety Lead Officer
- Network Manager
- Parents / Carers
- Children and Young People

6 Policy Statements

6.1 Policy Statements identify the areas of action and responsibility relevant to the identified individuals and groups. These statements represent the commitment of the establishment with regards to e-Safety and what it expects of the people who come under its remit. An example statement would be '*The [agency] will be responsible for ensuring that the technical infrastructure / network is as safe and secure as possible, and that policies and procedures approved within this policy are implemented. It will also ensure that the relevant people named in the above sections will be effective in carrying out their e-Safety responsibilities.*

- *All users will be provided with a username and complex password. Users will be required to change their password every 30 days.*
- *Users will be responsible for the security of their username and password in accordance with the Information Security and Computer Usage Policy, and the eBehaviour agreements (NB as appropriate to their setting, ie provision for SEN children and children with disabilities).*
- *The establishment has in place a filtering mechanism and associated policy to block and prevent identified harmful and inappropriate websites. The list is monitored and updated on a regular basis in line with best practice such as provided by the Internet Watch Foundation.*

7 Incident Management Process

7.1 The incident management process will be defined by the Local Authority and will be available as part of this policy pack. It is important that this is made available to all people within the establishment who may at any point come in contact with a child or young person.

8 Policy Pack

8.1 When developing appropriate policies, it is important that they are complementary and cover all appropriate areas. This set of guidelines should be read in conjunction with the following documents, which form the 'pack';

- BMBC Information Security and Computer Usage Policy
- BMBC Information Security and Computer Usage Protocols
- eBehaviour Agreement Guidance
- eSafety Policy
- Self Review Tool
- Social networking guidance

9 Further Information

9.1 If you require further support regarding any aspect of eSafety, you should contact your eSafety designated lead. In the event that this is not appropriate, you can email eSafety@barnsley.gov.uk or contact 01226 772400 in the first instance.

Revised June 2011