MSCB

MANCHESTER SAFEGUARDING
CHILDREN BOARD

E-SAFETY - GUIDELINES FOR MINIMUM STANDARDS

October 2009

Table of Contents

Introduction

"The introduction of these E- Safety minimum standards by the MSCB is a key step in progressing our shared responsibility of safeguarding children. The use of the Internet and digital technologies has developed at an astonishing rate and it is typically the case that the exciting benefits and opportunities presented have been more comfortably embraced by the young, rather than parents and other adults. With these benefits there come undoubted and significant threats. As Head of Crime Operations for one of the country's major cities I see the way in which the anonymity provided by digital communications is seized upon and manipulated by those seeking to use it for their own malevolent and predatory ends. Sadly, these types of incident are regularly coming to our attention, but the nature of these offenders is such that those instances that we are aware of are likely to be only a proportion of their true levels of offending. These minimum standards offer clear guidance and support for agencies in developing appropriate policies. We need to deploy a range of measures, both technical and policy based to combat the problem but the key measure has got to be the education of children and our staff. The oft used analogy is that swimming pools can be dangerous for children and whilst fencing, life-guards and signage can mitigate the risk, the most effective measure is to teach them to swim. The implementation of the these standards is the beginning of a process to ensure we provide the most effective protection and guidance possible for children in Manchester."

Mark Roberts -
Superintendent Crime Operations
North Manchester Division - Greater Manchester Police
E-Safety Lead MSCB

Policies and Procedures

It is MSCB policy that all member agencies must:

Appoint an E-safety Officer who will:

1. Serve as a single point of contact both for MSCB and agency staff and service users
2. Maintain and if necessary drive forward the creation of an E-safety policy (AUP)
3. Take responsibility for reviewing the AUP and relevant procedures at least annually and sooner in response to new technologies being used /analysis of logs and emerging trends.
4. Make appropriate responses to policy breaches and ensure correct execution of reporting procedures including escalating incidents with external agencies as appropriate.
5. Maintain logs for E-safety incidents and training provided to staff or service users

6. Take responsibility for providing or arranging staff training as appropriate. Above all, staff should be made aware that they have professional responsibilities for pupils' safety in this area.
7. Ensure that an E-safety education programme for children using technologies is in place.

NB. It is recommended that the E-safety Officer Role be given to a staff member who already has responsibility for safeguarding.

Make sure that an Acceptable Use Policy (AUP) is in place.

1. It will be necessary to have separate AUPs for staff and pupils. The AUP should cover the use of all technologies used.
2. The AUP must be appropriate to the age of the users and written in language that the user will understand.
3. Users (and /or) their designated carers should be required to sign the AUP.
4. The AUP should be reviewed regularly (at least every 12 months) and updated in line with developments in new technologies.
5. The AUP should clearly define what uses of the technology are acceptable (and those that are not.)
6. Sanctions for not complying with the AUP should be stated.
7. The AUP should state what monitoring and reporting of individual usage is in place.

When writing the policy agencies need to identify how breaches of the policy will be identified and recorded and additionally what action will be taken in response to an incident. (SEE MONITORING & REPORTING SECTION)

Becta has produced robust and comprehensive guidance (AUPs in Context), which although written for school and education establishments, could be used to inform the writing of an Acceptable Use Policy for any agency working with children or young people
This can be downloaded from
http://publications.becta.org.uk/display.cfm?resID=39286

Review and evaluate all internal policies and procedures

At least every twelve months or in response to new technologies or e-safety incidents if sooner.
This should be done in consultation with all stakeholders, including staff, volunteers, children, young people, parents and carers. The review should be recorded, setting out issues identified, action to be taken and responsibility for the actions.

Infrastructure and Technology

It is MSCB policy that all member agencies must:

Identify all technologies used within the agency itself.

Carry out risk assessments with regards to E-safety

On all technologies that children have access to. Risk assessment should look towards emerging issues and technologies in an attempt to pre-empt E-safety risks before they occur.

Use an ISP or filtering provider that subscribes to the IWF URL filtering list

(http://www.iwf.org.uk/public/page.148.htm) as a minimum.

URLs on the IWF URL filtering list contain potentially illegal content of child sexual abuse, but do not include potentially illegal content inciting racial hatred or any other inappropriate content. Additional filtering mechanisms must be employed to limit these risks, as ***appropriate to the users of the services*** in question.
Member agencies using a Becta accredited service or product will already benefit from a minimum level of filtering which includes the URLs on the IWF URL list.

Member agencies not using an accredited service or product should seek clarification from their ISPs or filtering providers on filtering criteria and performance, and should review and monitor their effectiveness accordingly.

It is recommended that all member agencies should:

Develop standards of ICT implementation in line with (or based on) Becta's functional and technical specifications.

(http://localauthorities.becta.org.uk/index.php?section=pf&catcode=ls_pict_04&offset=5&rows=5&orderby=1)

Use a Becta-accredited service for Internet connectivity and content filtering.

(http://schools.becta.org.uk/index.php?section=lv&&catcode=ss_lv_str_02&rid=13219) Member agencies should check the accreditation status of their ISP or filtering service and suggest investigating the possibility of accreditation if not already in place.

Consider the use of monitoring products

Member agencies must have their network infrastructure monitored regularly and consistently. There are now many software products available which can help with network monitoring, particularly tracking and identifying trends in advance of e-safety issues arising.

For guidance:

The Becta Accreditation of Internet Services to Education scheme (http://schools.becta.org.uk/index.php?section=lv&&catcode=ss_lv_str_02&rid=13219) enables schools and other establishments to make an informed choice of Internet service provider (ISP) or filtering solution. Accredited suppliers must meet and maintain specific standards in content filtering and service performance.

Under the Becta accreditation scheme, a product for filtering Internet content must meet or exceed the following requirements.

- There must be telephone and web-based support for all aspects of the service.
- The product must block 100 per cent of illegal material identified by the Internet Watch Foundation (IWF).
- The product must be capable of blocking 90 per cent of inappropriate content in each of the following categories:
    - Pornographic, adult, tasteless or offensive material
    - Violence (including weapons and bombs)
    - Racist, extremist and hate material
    - Illegal drug taking and promotion
    - Criminal skills, proxy avoidance and software piracy.
    - It must be possible to request (or make) amendments to the blocked content.

Education and Training

It is MSCB policy that all member agencies must:

Ensure that staff / service users have appropriate training:

Leaders, Managers and Strategists
All Leaders, managers and strategists should have training in E-safety awareness and also technical awareness. This should be extended to include how E-safety fits into and impacts upon other child safeguarding policies and procedures.

Designated E-safety officers
Training and support in order to carry out the responsibility of the role (see section 1 – Policies and Procedures) The Designated E-safety Officer will need training in E-safety awareness and also technical awareness. This should be extended to include how E-safety fits into and impacts upon other child safeguarding policies and procedures. Training in assessing the risks posed to children / risks posed by adults should also be undertaken. CEOP ambassador training is recommended as the E-safety officer also has a responsibility to cascade E-safety awareness training for staff.

Staff responsible for the education of children – school / education based personnel
All staff responsible for the education of children will need awareness raising, training on how to use and embed e-safety teaching materials into the curriculum. Half day CEOP 'Think U Know' training is recommended in order to help introduce staff to the technologies that children are using and the risks posed to children / risks posed by adults.
It is recommended that E-safety awareness / links to other safeguarding policies and procedures are incorporated into internal safeguarding staff training.

Staff working with children in contexts other than education
All staff working with children will require awareness raising on issues including:

1. What young people are doing online?
2. What are the risks?
3. Spotting warning signs
4. Accessing help and reporting incidents – how this links into existing safeguarding procedures.

Children / Young People
Appropriate E-safety awareness training incorporated into the curriculum through all key stages. E-safety education should include how to behave responsibly, how to use technology safely and how to report any concerns or incidents. All agencies should take any opportunity to re-enforce safety messages.

Parents & Carers

Parents and carers should be made aware of the agency's AUP (it is recommended that the parent / carer is required to sign to show they agree to the terms of the AUP) and also offered advice on where to find additional information / help on E-safety issues.

Technical / IT support staff

All technical staff should be aware of the issues. They should be fully aware of their proactive and reactive responsibilities for monitoring the network infrastructure in relation to e-safety.
Staff responsible for managing the technical infrastructure in each of the member agencies will need support in their roles. They will require regular training in e-safety issues, and should be clear about the procedures they must follow if they discover, or suspect, e-safety incidents through monitoring of network activity.
Infrastructure staff should understand the importance of maintaining logs, and securing and preserving the technical environment in order to be able to gather any evidence that may be required in the future. They should also know how to respond to requests for disclosure of information.

Ensure that logs are kept detailing training undertaken by staff and children

Ensure that a programme of refresher training is put in place to keep all staff / service users up to date with E-safety developments.

Monitoring and reporting

It is MSCB policy that all member agencies must:

Have their network infrastructure monitored regularly and consistently.

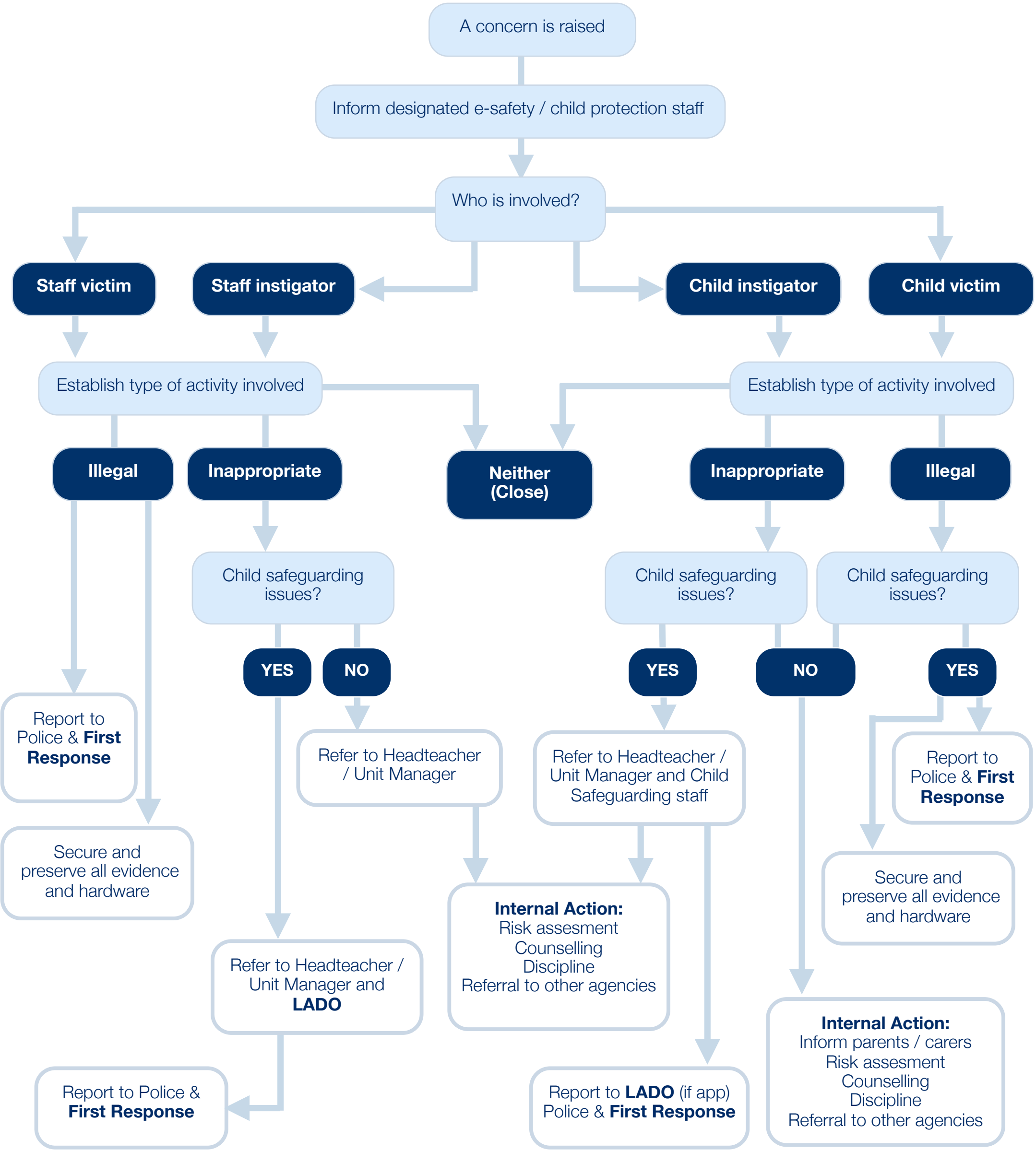
Maintain incident logs. These should include:

1. A description of the e-safety incident
2. Details of people involved.
3. How the incident was identified.
4. What actions were taken, and by whom.
5. Conclusions to the incident.

MSCB has produced a flowchart to show how to respond to an incident and where it would be appropriate to escalate an E-safety incident on to other agencies (see next page).

MSCB
MANCHESTER SAFEGUARDING CHILDREN BOARD

Incident Response Form



A concern is raised

Inform designated e-safety / child protection staff

Who is involved?

Staff victim

Staff instigator

Child instigator

Child victim

Establish type of activity involved

Establish type of activity involved

Illegal

Inappropriate

Neither (Close)

Inappropriate

Illegal

Child safeguarding issues?

Child safeguarding issues?

Child safeguarding issues?

YES

NO

YES

NO

YES

Report to Police & **First Response**

Secure and preserve all evidence and hardware

Refer to Headteacher / Unit Manager

Refer to Headteacher / Unit Manager and Child Safeguarding staff

Report to Police & **First Response**

Secure and preserve all evidence and hardware

Internal Action:
Risk assesment
Counselling
Discipline
Referral to other agencies

Refer to Headteacher / Unit Manager and **LADO**

Internal Action:
Inform parents / carers
Risk assesment
Counselling
Discipline
Referral to other agencies

Report to Police & **First Response**

Report to **LADO** (if app) Police & **First Response**

First Response Team	**- Telephone - 0161 255 8250**
Local Area Designated Officer	**- Telephone - 0161 203 2393**

In the event of a serious incident involving electronic media occurring within an agency, it is essential that a review of all e-safety and acceptable use policies and procedures be conducted as soon as possible. The senior manager responsible for the agency's operations would have ultimate responsibility for the review process, but may delegate this to the e-safety officer.

Annex

Recommended training:

CEOP ‘Think U Know” half day training and the CEOP Ambassador course.
www.thinkuknow.co.uk/teachers/training.aspx

Recommended teaching resources

The Child Exploitation and Online Protection Centre’s (CEOP) ‘Think U Know’ Programme.
DCSF / Childnet International Digizen training (anti-bullying).
Childnet ‘Know it All’ resources

Useful Documents & Websites

The following documents may be of use to member agencies

Safer Children in A Digital World – The Byron Review
(http://www.dcsf.gov.uk/byronreview/)

Becta – AUPs in Context
(http://publications.becta.org.uk/display.cfm?resID=39286*)*

Becta Framework for ICT Technical Support (FITS) and FITS Operations Management (FITS OM) set out the processes schools should have in place. FITS OM includes security administration as a process in its own right.
(http://schools.becta.org.uk/index.php?section=re&catcode=ss_res_tec_02)

Becta’s functional and technical specifications
(http://localauthorities.becta.org.uk/index.php?section=pf&catcode=ls_pict_04&offset=5&rows=5&orderby=1)
The functional specification sets out Becta’s vision for institutional infrastructure and considers school ICT from a functional perspective. It gives a detailed breakdown, under four broad headings of the features that schools should expect from the institution’s infrastructure; including ‘Using ICT to secure data and protect the user’.

Becta's Internet Services Accreditation
(http://localauthorities.becta.org.uk/index.php?section=pf&catcode=ls_pict_08)
The service enables schools (and others) to purchase internet services from accredited suppliers that meet and maintain specific standards in content filtering and service performance.

UK Access Management Federation
(http://localauthorities.becta.org.uk/index.php?section=pf&catcode=ls_pict_08)
This federation is a strategic approach to school web content

authentication and authorisation. Becta's work on securely accessing online content for the education sector should be adopted as an integral component in the strategic approach to the future development of ICT in education, skills and children's services. An overview report of Becta's work is available on the UK Access Management Federation website.

The National Education Network (NEN)

(http://schools.becta.org.uk/index.php?section=lv&catcode=ss_lv_saf_se_03&rid=12108)
It is envisaged that the NEN will provide every teacher and learner with access to a consistent set of resources, services and applications. Baseline standards for safety, security and functionality are being developed to support the NEN.