MSCB

MANCHESTER SAFEGUARDING CHILDREN BOARD

SAFEGUARDING ONLINE GUIDELINES FOR MINIMUM STANDARDS VERSION 3.0

January 2014

INTRODUCTION

This is the third version of the Manchester Safguarding Children Board Minimum Standards for E-safety. To reflect the integrated nature of the internet and mobile technology in all areas of safeguarding, this document has been renamed as 'MSCB Safeguarding Online – Minimum Standards'.

Recognising that not all agencies provide the same services or even have the same degree of contact with children and young people, this document sets the standards out according to the different types of settings MSCB encompasses, taking into consideration aspects such as direct contact with children and young people (CYP), provision of online access and responsibility for imparting education.

The appropriate section should therefore be chosen to establish the applicable minimum standard for each setting based on provision.

TABLE OF CONTENTS

1. NO DIRECT WORK WITH CHILDREN OR YOUNG PEOPLE

Where agencies do not work directly with children and young people, but there is a person responsible in some way for safeguarding children as part of the agency's remit, the following standards should be applied:

STANDARDS

1. **Ensure** that any people responsible for safeguarding receive training to raise awareness of the risks posed by the internet and mobile technologies to children and young people
2. **Update** all appropriate policies to include online safeguarding, detailing how to manage incidents and contact details for the agency safeguarding lead.
3. **Highlight** where further information and advice can be obtained if necessary

2. DIRECT WORK WITH CYP BUT NO ONLINE ACCESS

Where agencies work directly with children and young people, either on a regular basis or possibly settings which provide more transient provision (e.g. advice centres)but do not provide any equipment allowing access to the online world (either by means of actual devices such as laptops or tablets or by providing Wi-Fi access) then the following standards should be applied:

STANDARDS

1. **Ensure** that the person designated for safeguarding children undertakes the following responsibilities:
    a. Be the point of contact for service users and staff
    b. Be responsible for ensuring that the minimum standards as below are observed in the individual setting.
2. **Update** all appropriate policies to include online safeguarding including incident management and contact details for the agency safeguarding lead (this should be done at least every twelve months or in response to new technologies or e-safety incidents if sooner).
3. **Staff** must receive regular and appropriate training on safeguarding online:
    a. **Designated person with responsibility for safeguarding** should receive training promoting awareness of the risks posed by the internet and mobile technology, how to deal with incidents including escalation and reporting, and creation / maintenance of policy.
    b. **Staff working with children / young people** - Online safeguarding should be embedded into sessions provided on safeguarding where possible. All staff should be made aware of:
        - The risks posed by the online world;
        - Possible warning signs;
        - Who to go to if an incident occurs (for example a disclosure) and how this links into in-house safeguarding procedure;
        - Professional standards and protecting themselves (i.e. not friending children etc. on social network sites)and
        - The agency policy on the use of personal devices (i.e. phones, cameras etc.) onsite.
4. **Settings** should maintain an incident log, these should include:
    - A description of the safeguarding incident (including how online or communications technology was involved);
    - Details of the people involved;
    - How the incident was identified;
    - What actions were taken and by whom and
    - Conclusions to the incident.

An incident response chart and further guidance on handling an incident can be found on pages 9- 10.

NB - Settings working with vulnerable children and young people or where an issue has been identified - Where appropriate (for example in support groups or settings working with vulnerable children) build in appropriate educational sessions concerning online issues for children and staff (this may include specific information on the role of the online world in self harm, sexual exploitation and bullying).

3. DIRECT WORK WITH CYP AND ONLINE ACCESS FOR STAFF ONLY

Where settings work directly with children or young people and internet access is provided for staff only, the following standards apply:

STANDARDS

1. **Ensure** that the person designated for safeguarding children undertakes the following responsibilities:
    a. Be the point of contact for service users and staff
    b. Be responsible for ensuring that the minimum standards as below are observed in the individual setting.
2. **Update** all appropriate policies to include online safeguarding including incident management and contact details for the agency safeguarding lead (this should be done at least every twelve months or in response to new technologies or e-safety incidents if sooner).
3. **Staff** must receive regular and appropriate training on safeguarding online**:**
    a. **Designated person with responsibility for safeguarding** should receive training promoting awareness of the risks posed by the internet and mobile technology, how to deal with incidents including escalation and reporting, and creation / maintenance of policy.
    b. **Staff working with children / young people -** Online safeguarding should be embedded into sessions provided on safeguarding where possible. All staff should be made aware of:
        - The risks posed by the online world;
        - Possible warning signs;
        - Who to go to if an incident occurs (for example a disclosure) and how this links into in-house safeguarding procedure;
        - Professional standards and protecting themselves (i.e. not friending children etc. on social network sites) and
        - The agency policy on the use of personal devices (i.e. phones, cameras etc.) onsite.
4. **Settings should maintain an incident log**, these should include:
    - A description of the safeguarding incident (including how online or communications technology was involved);
    - Details of the people involved;
    - How the incident was identified;
    - What actions were taken and by whom and
    - Conclusions to the incident.
5. **Acceptable use policies**[1] for staff should be produced.

An incident response chart and further guidance on handling an incident can be found on pages 9 - 10.

NB - Settings working with vulnerable children and young people or where an issue has been identified - Where appropriate (for example in support groups or settings working with vulnerable children) build in appropriate educational sessions concerning online issues for children and staff (this may include specific information on the role of the online world in self harm, sexual exploitation and bullying).

[1] See page 12

4. DIRECT WORK WITH CYP, ONLINE ACCESS FOR STAFF AND CYP

Where settings work directly with children or young people and internet access is provided for staff AND children or young people, the following standards apply:

STANDARDS

1. **Ensure** that the person designated for safeguarding children undertakes the following responsibilities:
    a. Be the point of contact for service users and staff
    b. Be responsible for ensuring that the minimum standards as below are observed in the individual setting.
2. **Update** all appropriate policies to include online safeguarding including incident management and contact details for the agency safeguarding lead (this should be done at least every twelve months or in response to new technologies or e-safety incidents if sooner).
3. **Staff** must receive regular and appropriate training on safeguarding online:
    a. **Designated person with responsibility for safeguarding** should receive training promoting awareness of the risks posed by the internet and mobile technology, how to deal with incidents including escalation and reporting, and creation / maintenance of policy.
    b. **Staff working with children / young people -** Online safeguarding should be embedded into sessions provided on safeguarding where possible. All staff should be made aware of:
        - The risks posed by the online world;
        - Possible warning signs;
        - Who to go to if an incident occurs (for example a disclosure) and how this links into in-house safeguarding procedure;
        - Professional standards and protecting themselves (i.e. not friending children etc. on social network sites)and
        - The agency policy on the use of personal devices (i.e. phones, cameras etc.) onsite.

    c. **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.

    d. **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.

e. **Children / young people -** 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.

4. **Settings should maintain an incident log,** these should include:
   - A description of the safeguarding incident (including how online or communications technology was involved);
   - Details of the people involved;
   - How the incident was identified;
   - What actions were taken and by whom and
   - Conclusions to the incident.

5. **Ensure that appropriate acceptable use policies (AUPs[2])** are in place for staff AND children.

6. **Identify all technologies used within the setting and carry out risk assessments with regards to online 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.

7. **Use an internet service provider or filtering product that subscribes to the Internet Watch Foundation URL filtering list[3].** URLs on the IWF URL (web address) filtering list contain potentially illegal content, but do not include lesser potentially inappropriate content. Additional filtering mechanisms must be employed to limit these risks, **as *appropriate to the users of the services*** in question.

8. **Use up-to-date security software / solutions -** All settings providing access to the online environment should satisfy themselves that their equipment is protected adequately against threats such as hacking, viruses and trojans.
   Agencies which allow personal data to be stored on mobile devices should ensure the use of appropriate encryption to protect it.

9. **Monitor network usage -** Member agencies should 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. The more sophisticated products can also provide feedback to the user and reinforce education about safe use.

10. **Ensure personally identifiable logons (including a secure password) are provided to all people using the access.** An incident response chart and further guidance on handling an incident can be found on pages 9 - 10.

NB - Settings working with vulnerable children and young people or where an issue has been identified - Where appropriate (for example in support groups or settings working with vulnerable children) build in appropriate educational sessions concerning online issues for children and staff (this may include specific information on the role of the online world in self harm, sexual exploitation and bullying).

[2] See page 12
[3] http://www.iwf.org.uk/members/member-policies/url-list

5. SCHOOLS AND EDUCATIONAL SETTINGS

Settings with a responsibility to provide general education for children and young people (e.g. schools and alternative provision) should apply the following standards.

STANDARDS

1. **Ensure** that the person designated for safeguarding children undertakes the following responsibilities:
    a. Be the point of contact for service users and staff
    b. Be responsible for ensuring that the minimum standards as below are observed in the individual setting.
2. **Update** all appropriate policies to include online safeguarding including incident management and contact details for the agency safeguarding lead (this should be done at least every twelve months or in response to new technologies or e-safety incidents if sooner).
3. **Staff** must receive regular and appropriate training on safeguarding online:
    a. **Designated person** with responsibility for safeguarding should receive training promoting awareness of the risks posed by the internet and mobile technology, how to deal with incidents including escalation and reporting, and creation / maintenance of policy.
    b. **Staff working with children / young people -** Online safeguarding should be embedded into sessions provided on safeguarding where possible. All staff should be made aware of:
        - The risks posed by the online world;
        - Possible warning signs;
        - Who to go to if an incident occurs (for example a disclosure) and how this links into in-house safeguarding procedure;
        - Professional standards and protecting themselves (i.e. not friending children etc. on social network sites) and
        - The agency policy on the use of personal devices (i.e. phones, cameras etc.) onsite.
    c. **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.

    d. **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.
4. **Incorporate E-safety into the curriculum -** Appropriate education programmes addressing safety online should be incorporated into the curriculum through all key stages within schools and educational settings. 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 every opportunity to re-enforce safety messages.

5. **Settings** should maintain an incident log, these should include:
   - A description of the safeguarding incident (including how online or communications technology was involved);
   - Details of the people involved;
   - How the incident was identified;
   - What actions were taken and by whom and
   - Conclusions to the incident.
6. **Ensure** that appropriate acceptable use policies (AUPs[4]) are in place for staff AND children.
7. **Identify** all technologies used within the setting and carry out risk assessments with regards to online 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.
8. **Use** an internet service provider or filtering product that subscribes to the Internet Watch Foundation URL filtering list[5]. URLs on the IWF URL (web address) 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.
9. **Use** up-to-date security software / solutions - All settings providing access to the online environment should satisfy themselves that their equipment is protected adequately against threats such as hacking, viruses and Trojans.
   Agencies who allow personal data to be stored on mobile devices should ensure the use of appropriate encryption to protect it.
10. **Monitor** network usage - Member agencies should 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. The more sophisticated products can also provide feedback to the user and reinforce education about safe use.
11. **Ensure** personally identifiable logons (including a secure password) are provided to all people using the access.

An incident response chart and further guidance on handling an incident can be found on pages 9 - 10.

NB - Settings working with vulnerable children and young people or where an issue has been identified - Where appropriate (for example in support groups or settings working with vulnerable children) build in appropriate educational sessions concerning online issues for children and staff (this may include specific information on the role of the online world in self harm, sexual exploitation and bullying).

In addition:

Ofsted

Schools will be aware that these are minimum standards laid down by the LSCB. Schools should also be aware of the expectations of Ofsted with respect to online safety[6].

[4] See page 12
[5] http://www.iwf.org.uk/members/member-policies/url-list
[6] http://www.ofsted.gov.uk/resources/briefings-and-information-for-use-during-inspections-of-maintained-schools-and-academies-september-2

6. RESPONDING TO INCIDENTS

Incidents raising safeguarding concerns - Any incidents that raise safeguarding concerns should be handled by the designated person and the MSCB safeguarding procedures should be implemented. This includes undertaking reports to Children's Services – Contact Centre and the Police as appropriate.

Where a member of staff is involved in this, a referral to the Local Area Designated Officer (LADO) should be made.
The following incidents must always be reported to the Police.

- Discovery of indecent images of children and young people;
- Behaviour considered to be 'grooming';
- Sending of obscene materials.

Incidents involving illegal content - On discovery of illegal content, the equipment or materials found should not be tampered with and advice should be sought from the Police. Computers or other devices should not be switched off unless instructed to do so by the Police. Further access to the illegal content should be prevented by keeping other people out of the area. If necessary the monitor itself can be turned off but the computer should remain as you have found it (DO NOT shut the machine down).

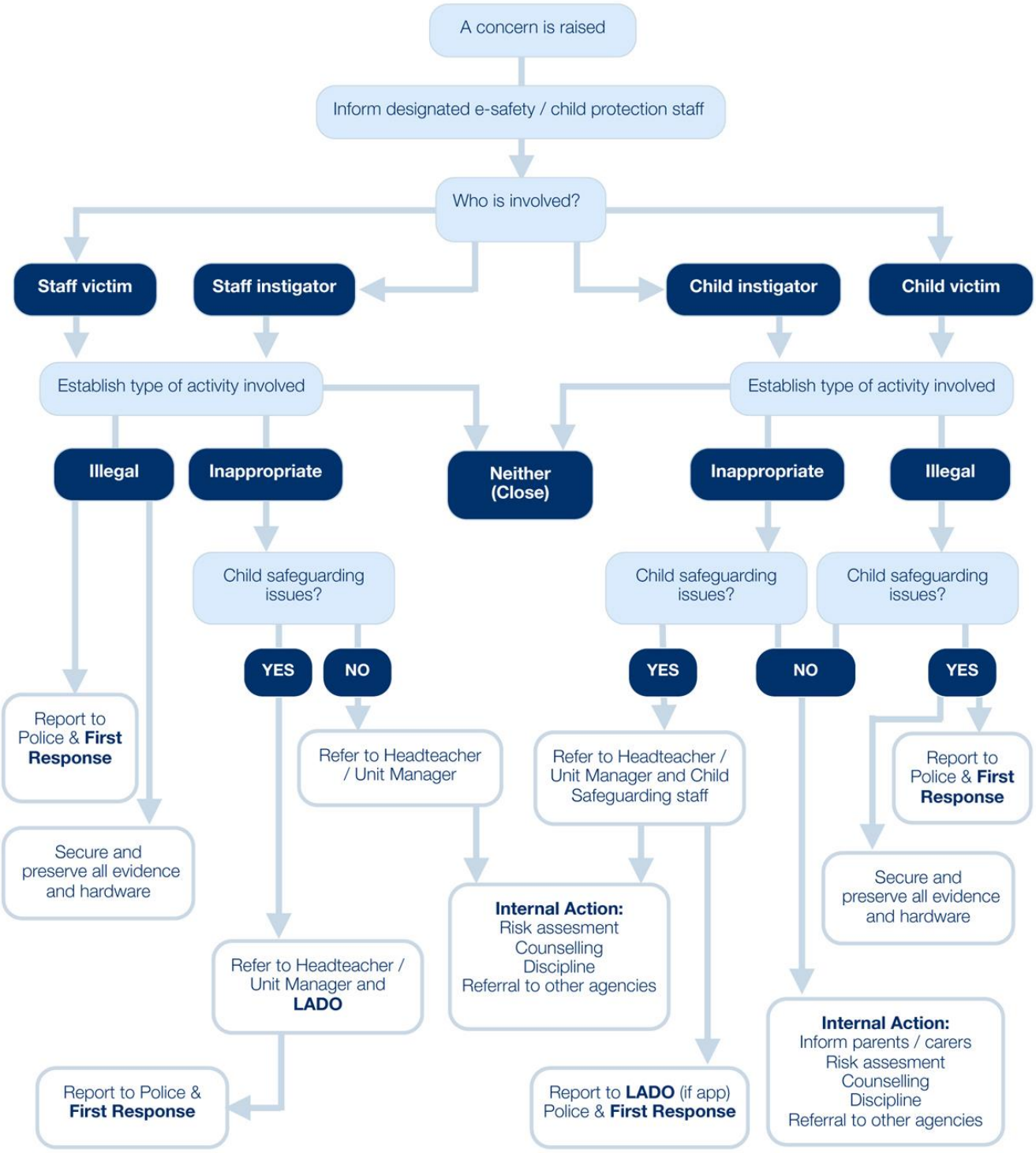
No attempt should be made to download, print or send any materials found. (By doing so you may commit further offences)

All illegal content must be reported to the Police and the Internet Watch Foundation (www.iwf.org.uk)

Incident Response Form – See over page

MSCB
MANCHESTER SAFEGUARDING CHILDREN BOARD

Incident Response Form



First Response Team - Telephone - **0161 234 5001**
Local Area Designated Officer - Telephone - **0161 274 6555**

Undertake reviews following serious incidents.

In the event of a serious incident involving access to the internet / mobile technology occurring within an agency, it is essential that a review of all relevant policies and procedures be conducted as soon as possible. The senior manager responsible for the agency's operations has ultimate responsibility for the review process, but may delegate this to the designated person for safeguarding.

7. EXPLANATORY NOTES

For settings where AUPs are required:

Acceptable use policies (AUPs)/ agreements should be promoted amongst staff and service users.

- Where both staff and CYP are allowed access, it will be necessary to have separate AUPs for staff and pupils. The AUP should cover the use of all technologies used.
- The AUP must be appropriate to the age of the users and written in language that the user will understand.
- Users (and /or) their designated carers must be made aware of the contents of the AUP and that any use of the setting access is allowed only subject to adherence to the policy.
- The AUP should be reviewed regularly (at least every 12 months) and updated in line with developments in new technologies.
- The AUP should clearly define what uses of the technology are acceptable (and those that are not.)
- Sanctions for not complying with the AUP should be stated.
- 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 responding to incidents section)

Designated person – Person within individual settings designated as the person responsible for safeguarding.

IIOC – Indecent image of children

CYP – Child or young person

Self generated indecent image (SGII) – indecent photograph or video taken by the child or young person themselves.

8. FURTHER ADVICE

CEOP – Child Exploitation Online Online Protection Centre www.ceop.police.gov.uk
Think U Know resources for teachers, trainers and children www.thinkuknow.co.uk
Digizen - Information on Cyberbullying and Social Networks www.digizen.org

Beat Bullying (formerly Cybermentors) - Staffed by trainined YP, Beat Bullying provide a service to support and listen to YP who are being bullied. The cybermentors are supported by BACP accredited counsellors. http://www.beatbullying.org/

IWF – The Internet watch Foundation is the UK internet Hotline for the public and IT professionals to report criminal online content in a secure and confidential way. www.IWF.org.uk

MSCB Sexting Guidance Document – Additional guidance for understanding and responding to incidents where young people create and / or circulate indecent images of themselves / other young people. (shortly to be released)

Online Safety Compass - Online Compass is a free online safety self review tool for any group that works with children and young people. www.onlinecompass.org.uk/

Professionals Online Safety Helpline - Free advice for professionals working with children and young people on all areas of online safety. www.saferinternet.org.uk/helpline

UK Safer Internet Centre - The latest advice on how to use the internet and new technologies safely and responsibly. Also find a range of practical resources, news and events focussing on the safe and responsible use of the internet and new technologies. www.saferinternet.org.uk/

360 Degree Safe - The 360 degree safe self review tool is currently available free of charge and is intended to help schools review their eSafety policy and practice - www.360safe.org.uk/