

**OLDHAM LOCAL SAFEGUARDING CHILDREN BOARD**  
**E-SAFETY POLICY & GUIDANCE**

## **1 Introduction**

1.1 This policy provides guidance on effective approaches to e-safety for agencies in Oldham.

1.2 It covers:

- Awareness raising for children and young people, so that they are able to keep themselves as safe as possible when using the internet and other digital technologies.
- The policies and procedures to enable agencies to support the e-safety of children and young people. .
- The responses necessary when a risk to a child is discovered.

1.3 The focus of this policy is to ensure that existing policies (such as those on child protection, bullying, the curriculum, and behaviour) are applied to the digital environment. In order for this to happen, it is essential that these policies are regularly reviewed against this e-safety guidance, and updated as necessary.

1.4 This policy should be read in line with the Greater Manchester Safeguarding Children Board procedures  
<http://www.gmsafeguardingchildren.co.uk/procedures/concerns-about-adults/>

1.5 Safeguarding children, including e-safety is everyone's responsibility; e-safety is not a responsibility for just IT staff.

## **2 Background**

2.1 As part of the Every Child Matters agenda set out by the Government, (Education Act 2002 and the Children Act 2004), states it is the duty of organisations to ensure that children and young people are protected from potential harm. In order to do this, we need to involve children and young people and their parent / carers in the safe use of on-line technologies. The term 'e-safety' is used to encompass the safe use of all on-line technologies in order to protect children, young people and adults from potential and known risks.

2.2 It is important that adults who work with children are clear about safe practices, so that they are safeguarded from misunderstanding or possible allegations of inappropriate behaviour, for example, only contacting children and young people about homework via a school e-mail address, not a personal one.

2.3 Unfortunately it is not possible to create a 100% safe environment and it is the organisations responsibility to demonstrate that they have managed the risks and have done everything that they reasonably

could in order to protect the children and young people they work with. Organisations require policies and procedures that are clear and easy to follow so that risks are minimised and any incidents that do occur can be dealt with quickly and effectively.

2.4 In addition to accessing the internet through organisations that work with children, young people will use the internet and other digital technology in their own time at other locations and are at greater risk **if** they have not been taught what the dangers are and how to use them safely. Supporting and assisting the development of children and young people's e-confidence and their ability to access the digital world effectively and safely is important to all organisations.

2.5 It is important to recognise that the range of risks to young people in the digital environment is wide and ever-changing. 'Grooming' by sexual predators via internet-enabled multi-player games is not uncommon.

### **3 The Oldham Charter of Young People's Digital Rights**

3.1 The Oldham Local Safeguarding Children Board (LSCB) supports the Charter of Young People's Digital Rights developed by the Oldham Youth Council, because:-

- A key element of child protection in the digital environment is developing the skills and confidence of young people in the face of threats to their safety, enabling them to adopt the safest possible behaviours themselves and to be able to report situations and behaviours of others that could constitute a threat. These messages are more likely to be adopted and taken to heart by children and young people if presented in terms of their own rights than if presented as a set of rules about what they shouldn't do.
- E-safety is a safeguarding issue and all organisations need to review their existing procedures to ensure that e-safety is incorporated into these rather than being a stand alone procedure.

3.2 **Youth Council Charter of Young Peoples Digital Rights can be found by following this link <http://www.esafetyweek.info/>**

3.3 Organisations are encouraged to promote the Charter and the CEOP report abuse button [http://www.ceop.gov.uk/ceop\\_report.aspx](http://www.ceop.gov.uk/ceop_report.aspx) , ensuring it is displayed wherever young people use technology such as:

- Learning Platforms and Virtual Learning Environments
- Computers in youth centres, clubs, schools, libraries and the City Learning Centre
- Student planners and homework diaries
- School Websites

- 3.4 The Charter could also feature as part of e-safety education within citizenship, PSHE and ICT.

#### **4 Acceptable Use Policies**

4.1 All organisations providing internet access for young people should have an Acceptable Use Policy (AUP), which sets out the roles, responsibilities and procedures for the acceptable, safe and responsible use of on-line technologies. This will help safeguard adults, children and young people within these settings. The AUP should detail how organisations will provide support and guidance to parents / carers and the wider community for the safe and responsible use of these technologies by adults, children or young people. AUPs are typically about both child protection and how to use the computers.

4.2 It may be appropriate to develop a number of documents as part of the AUP for different audiences:

- Management
- Staff / Volunteers
- Children and Young People
- Parents

#### **5 The E-Safety Lead**

5.1 It is important to have a lead e-safety person within each organisation whose main roles and responsibilities should include:

- Updating the AUP
- Ensuring that the organisation's policies and procedures include aspects of e-safety for example the anti-bullying procedure includes cyber-bullying. Child protection policy to include internet grooming.
- Work with the Network Manager / filter system provider to ensure that the filtering is set at the correct level for staff, children and young people
- Report issues to the head of the organisation
- Ensure staff training is provided on new emerging e-safety issues
- Ensure e-safety is included in staff induction
- Monitor and evaluate incidents that occur to inform future safeguarding developments.

#### **5.2 Allegation Procedures and the Child Protection Procedure**

5.2.1 The procedure for managing allegations against adults who work with children and young people

([http://www.oldham.gov.uk/manging\\_allegations\\_against\\_adults\\_who\\_work\\_with\\_children-2.pdf](http://www.oldham.gov.uk/manging_allegations_against_adults_who_work_with_children-2.pdf)) should also include incidents that occur as a result of using digital technologies, which may result in an allegation of misuse or misconduct being made against a member of staff or volunteer. All allegations should be reported to the Local Authority Designated Officer 0161 770 8870.

## **6 Appendix One**

### **6.1 Information and websites about e-safety.**

#### 6.1.1 CEOP

- <http://www.ceop.gov.uk/>

#### 6.1.2 Think U Know

- <http://www.thinkuknow.co.uk/Default.aspx?AspxAutoDetectCookieSupport=1>

#### 6.1.3 Becta

- <http://localauthorities.becta.org.uk/index.php?section=esf>

#### 6.1.4 Childnet

- <http://www.childnet-int.org/>

#### 6.1.5 Internet Watch Foundation

- <http://www.iwf.org.uk/>

## **7 Appendix Two**

### **7.1 Sample Procedure (to be incorporated into existing procedures)**

7.1.1 The manager of the organisation will ensure that an adult follows these procedures in the event of any misuse of the internet:

#### **7.2 An inappropriate website is accessed inadvertently:**

- Report website to the e-safety lead.
- Contact the filtering service so that the site can be added to the banned or restricted list.
- Change Local Control filters to restrict locally.
- Log the incident.

#### **7.3 An inappropriate website is accessed deliberately:**

- Ensure that no one else can access the material by shutting down the computer.
- Log the incident.
- Report to the manager and e-Safety lead immediately.

- Manager to refer back to the Acceptable Use Rules and follow agreed actions for discipline.
- Inform the filtering services as with 9.2 in order to reassess the filters.

**7.4 An inappropriate website is accessed deliberately by a child or young person:**

- Refer the child to the Acceptable Use Rules that were agreed.
- Reinforce the knowledge that it is illegal to access certain images and police can be informed.
- Log the incident
- Decide on appropriate sanction.
- Notify the parent/carer.
- Contact the filtering service to notify them of the website.

**7.5 An adult receives inappropriate material:**

- Do not forward this material to anyone else – doing so could be an illegal activity.
- Alert the manager immediately.
- Ensure the device is removed and log the nature of the material.
- Contact relevant authorities for further advice e.g. police, social care CEOP.
- Log the incident

**7.6 An illegal website is accessed or illegal material is found on a computer.**

**7.6.1 The following incidents must be reported directly to the police (add number):**

- Indecent images of children found. (Images of children whether they are photographs or cartoons of children or young people apparently under the age of 16, involved in sexual activity or posed in a sexually provocative manner)
- Incidents of 'grooming' behaviour.
- The sending of obscene materials to a child.
- Criminally racist or anti-religious material
- Violent or bomb-making material
- Software piracy
- The promotion of illegal drug-taking

- Adult material that potentially breaches the obscene publications act in the UK.

7.6.2 If any of these are found, the following should occur:

- Alert the manager / e-safety lead immediately.
- **DO NOT LOG OFF** the computer but disconnect from the electricity supply.
- Contact the police and or CEOP and social care immediately (Police - 0161 856 8962, social care -0161 770 3790, children over 16 - 0161 770 6599, out of hours - 0161 770 6936).
- If a member of staff or volunteer is involved, refer to the allegations against staff policy and report to the Local Authority Designated Officer.

**7.7 An adult has communicated with a child or used ICT equipment inappropriately (e-mail/ text message etc)**

- Ensure the child is reassured and remove them from the situation.
- Report to the manager and Designated Person for Child Protection immediately, who will then follow the Allegations Procedure and Child Protection Procedures [www.oldham.gov.uk/lscb-home](http://www.oldham.gov.uk/lscb-home) .
- Report to the Local Authority Designated Officer (add contact number).
- Preserve the information received by the child if possible.
- Contact the police as necessary.

**7.8 Threatening or malicious comments are posted to the school website or learning platform (or printed out) about an adult in school:**

- Preserve any evidence and log the incident.
- Inform the manager immediately and follow Child Protection Policy.
- Inform the e-Safety Leader so that new risks can be identified.
- Contact the police or CEOP if appropriate.

**8** Where staff or adults are posted on inappropriate websites or have inappropriate information about them posted this should be reported to the manager.

**8.1** Threatening or malicious comments are posted to the school website or learning platform about a child in school or malicious text messages are sent to another child/young person (cyber bullying).

- Preserve any evidence and log the incident.
- Inform the manager immediately.
- Check the filter if an internet based website issue.
- Contact/parents and carers
- Refer to the bullying policy
- Contact the police or CEOP as necessary.

## **9** Appendix Three

### **9.1** AUP's

9.1.1 In order to prevent inappropriate situations occurring it is important that staff and children are aware of their responsibilities and the expectations whilst using technology. It would be good practice to have each child or young person sign and date the policy and send a copy to each young/person and their carers.

9.1.2 Exemplar to be agreed and discussed by Individual Management Teams

9.1.3 Acceptable Use Policy for Staff

- I know that I should only use the school equipment in an appropriate manner.
- I know that images should not be inappropriate or reveal any personal information of children and young people if uploading to the Internet.
- I have read the Procedures for Incidents of Misuse so that I can deal effectively with any problems that may arise.
- I will report accidental misuse.
- I will report any incidents of concern for children or young people's safety to the Head teacher/manager, Designated Person for Child Protection or e-Safety Leader in accordance with the Acceptable Use Policy.
- I know who my Designated Person is for Child Protection.

I know that I am putting myself at risk of misinterpretation and allegation if I contact children and young people via personal

technologies, including my personal e-mail and phone and should use the school e-mail and phones (if provided) and only to a child's school e-mail address if possible .

- I know that I should not use the school IT system for personal use unless the Head teacher/manager and/or e-Safety Leader have agreed this.
- I know that I should complete virus checks on my laptop and memory stick or other devices so that I do not inadvertently transfer viruses, especially where I have downloaded resources.
- I will only install hardware and software I have been given permission for.
- I will ensure that I follow the Data Protection Act 1998.
- I will ensure that I keep my password secure and do not disclose any security information unless to appropriate personnel. If I feel someone inappropriate requests my password I will check with the e-Safety Leader.
- I have been given a copy of the Acceptable Use Policy to refer to about all e-safety issues and procedures that I should follow.
- I am aware that my e-mails and internet use may be monitored.
- I will adhere to copyright and intellectual property rights.

## **10 Appendix Four**

### **10.1 Legal framework**

10.1.1 This section is designed to inform users of legal issues relevant to the use of Communications. It is not professional advice.

10.1.2 Many young people and indeed some staff use the Internet regularly without being aware that some of the activities they take part in are potentially illegal. The law is developing rapidly and recent changes have been enacted through:

### **10.2 The Sexual Offences Act 2003,**

10.2.1 The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an Offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence.

10.2.2 Causing a child under 16 to watch a sexual act is illegal, including looking at images, such as videos, photos or web cams, for your own gratification.

10.2.3 It is also an offence for a person in a position of trust to engage in sexual activity with

10.2.4 Any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff fall in this category of trust).

10.2.5 Any sexual intercourse with a child under the age of 13 commits the offence of rape.

10.2.6 More information about the 2003 Act can be found at [www.teachernet.gov.uk](http://www.teachernet.gov.uk)

### **10.3 Communications Act 2003 (section 127)**

10.3.1 Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment.

10.3.2 This wording is important because an offence is complete as soon as the message has been sent, there is no need to prove any intent or purpose.

### **10.4 Data Protection Act 1998**

10.4.1 The Act requires anyone who handles personal information to notify the Information Commissioner's Office of the type of processing it administers, and must comply with important data protection principles when treating personal data relating to any living individual. The Act also grants individuals rights of access to their personal data, compensation and prevention of processing.

### **10.5 The Computer Misuse Act 1990 (sections 1 – 3)**

10.5.1 Regardless of an individual's motivation, the Act makes it a criminal offence to:

- I gain access to computer files or software without permission (for example using someone else's password to access files); I gain unauthorised access, as above, in order to commit a further criminal act (such as fraud); or I impair the operation of a computer or program (for example caused by viruses or denial of service attacks).

10.5.2 UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

### **10.6 Malicious Communications Act 1988 (section 1)**

10.6.1 This legislation makes it a criminal offence to send an electronic message (e-mail) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.

### **10.7 Copyright, Design and Patents Act 1988**

10.7.1 Copyright is the right to prevent others from copying or using his or her "work" without permission.

10.7.2 The material to which copyright may attach (known in the business as “work”) must be the author’s own creation and the result of some skill and judgement. It comes about when an individual expresses an idea in a tangible form. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer.

10.7.3 It is an infringement of copyright to copy all or a substantial part of anyone’s work without obtaining the author’s permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else’s material.

10.7.4 It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.

## **10.8 Public Order Act 1986 (sections 17 – 29)**

10.8.1 This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material, which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

## **10.9 Protection of Children Act 1978 (Section 1)**

10.9.1 It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

## **10.10 Obscene Publications Act 1959 and 1964**

10.10.1 Publishing an “obscene” article is a criminal offence. Publishing includes electronic transmission.

## **10.11 Protection from Harassment Act 1997**

10.11.1 A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other.

10.11.2 A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

## **11 Regulation of Investigatory Powers Act 2000**

11.1.1 The Regulation of Investigator Powers Act 2000 (RIP) regulates the interception of communications and makes it an offence to intercept or monitor communications without the consent of the parties involved in

the communication. The RIP was enacted to comply with the Human Rights Act 1998.

11.1.2 The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, however, permit a degree of monitoring and record keeping, for example, to ensure communications are relevant to school activity or to investigate or detect unauthorised use of the network. Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored.

11.1.3 Covert monitoring without informing users that surveillance is taking place risks Breaching data protection and privacy legislation.