OLDHAM LOCAL SAFEGUARDING CHILDREN BOARD

eSafety Policy and Guidance

Introduction

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

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.

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.

4 This policy should be read in conjunction with Oldham LSCB's other safeguarding policies and procedures.

Background

5 The Education Act 2002 and Children Act 2004 state that 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 parents / 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.

6 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).

7 All settings that work with young people should recognise that young people face a *range* of risks through their online activity, and should not focus only the the most high-profile risks.

8 It is useful to think of risks in terms of those associated with online *content*, from *contact*, and from *conduct*. The risks to children and young people broadly arise from the categories of:

- being misled (to the detriment of the child's health, socialisation, etc)
- being contacted (eg by bullies, paedophiles)
- being drawn into inappropriate conduct

The Oldham Charter of Young People's Digital Rights

9 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 asserting their own positive rights than if presented as a negative set of rules about what they shouldn't do.
- The charter provides a clear focus on the impact on the child of their whole experience online and their knowledge of how to adopt safe behaviours. This is valuable in ensuring that the approach taken in settings is not just about the internet access *provided by* the setting. (This is also in accordance with, for example, the best practice described for schools in the 2010 Ofsted report on esafety).

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

11 Organisations are encouraged to promote the Charter and the CEOP report abuse button 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

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

Acceptable Use Policies

13 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. It would not be good practice, however, for this AUP to be the centre of the setting's esafety approach - an AUPs' scope tends to be limited to the internet access *within* the setting and AUPs very often include measures to protect the computers from the children alongside those that are about child protection. An AUP is never a subsitute for a proper esafety policy.

14 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

The eSafety Lead and the Child Protection Lead

15 The child protection lead is often the best person to be the esafety lead, but where a separate role exists these two people should work closely together. eSafety is about child protection, not about ICT.

16 The role would include:

- Ensuring that the organisation's policies and procedures include e-safety - for example the anti-bullying procedures including cyber-bullying, the child protection procedures including internet grooming.
- Working with technical support to ensure that the filtering is set at the correct level for staff, children and young people, but also that filtering is not used as a substitute for education.
- Reporting issues to the head of the organisation.
- Ensuring that staff training is provided on new emerging e-safety issues and that esafety is included in staff induction.
- Ensuring that esafety education is comprehensive, age-related and effective.
- Monitor and evaluating incidents that occur to inform future safeguarding actions.

Professionals compromised or at risk of misinterpretation or false allegations as a result of contact through social networking

17 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) includes 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.

18 All allegations should be reported to the Local Authority Designated Officer 0161 770 8870.

19 To avoid false allegations, and to reduce the possibility of deliberate offending action, the following guidelines should be followed.

Use of Social Networking with Children and Young People

20 Social Networking can have great value as an educational and engagement tool with young people, but its use can also involve risks both to the young people themselves and to the adults working with them. Its use therefore should always be within the framework of these guidelines and policy.

21 The rapid growth of use of social networking among children and young people and its use at a younger and younger age means that all professionals working with young people should have some understanding of the key features of the most common social networking sites. Professionals working in a safeguarding capacity or with particularly vulnerable young people are likely to require a more detailed knowledge.

22 Specific risks associated with social networking include:

- professionals compromised or at risk of misinterpretation or false allegations as a result of contact through social networking
- professionals personal lives exposed to young people with whom they work in such a way as to compromise the effectiveness of their work
- young people sharing with strangers personal details of their lives (such as routes to and from school, usual places to hang about, home address, current location, etc)
- young people accepting as friends people posing as other young people, as celebrities, etc
- squabbles and fallings out of friends (that form a normal part of growing up) being played out in front of an online audience - with the facility for that audience to join in, comment, and cause the falling out to spiral out of control.
- cyber-bullying and other forms of conflict
- children and young people sharing images that they would not wish to enter into the public domain, then unable to get them back

19. Adults who work with children or young people in a professional or volunteer capacity should never have any of those children as friends on a personal account on Facebook or any similar social networking sites. To befriend a child on such a site provides that child with access to any personal details posted by the adult (including personal information about the adult's own adult friends) as well as providing the adult with similar personal details about the child and their friends. Such 'friending' on Facebook is not in accordance with the usual standards of professional conduct expected of professionals working with young people and promoted by their trades unions and professional bodies; it is comparable to inviting young people into the professionals home on an evening that they have all their friends round.

20. The appropriate response to any former pupil (or child or other young person *previously* worked with) making a friend request will be different in different settings according to the age and the nature of the setting. It would clearly be inappropriate, for example, for a teacher in a primary school to accept a friend request from a former pupil for many years. Even with older former students (post-18) the possibility must be considered that the former student may have younger friends or siblings still in the school as friends within their network, making the accepting of a friend request inappropriate in these circumstances too. Employers are expected to make their policy on this clear to staff.

21. Wherever Facebook or similar social networking site is being used by a professional with young people that must be with an account set up for the purpose that is entirely separate to any personal account that adult may have. Use must adhere to the following guidelines.

- Consideration should first be given to whether the presence on Facebook is best as a *person*, a *page* or a *group*. These different forms of presence have different impacts on information shared and made accessible by the young people engaged. (Detailed advice on this is available from the City Learning Centre).
- The LSCB eSafety Subgroup must be notified of the particular use of social networking via the LSCB manager, to be formally minuted at a Sub-Group meeting. This is a protection to staff as well as a register of usage.
- All staff involved must themselves have enhanced CRB clearance, and must have received eSafety

training from the LSCB Sub-Group or someone authorised by the Sub-Group as a trainer.

- Log-in details (passwords, etc) must be known to at least two different staff involved. (This is also a protection to staff against the possibility of any false allegations or compromising circumstances).
- Staff must ensure that e-safety knowledge and skills are promoted within or alongside use of the site, such as the 'click CEOP' button, the Oldham Charter of Young People's Digital Rights, and any privacy skills specific to the particular social networking site used.
- Staff must ensure that positive online citizenship is promoted, and any occurrences of cyber-bullying are appropriately acted upon.
- No other adults may be accepted as friends on this account (except professionals working alongside or monitoring usage, to whom all the same requirements apply).
- Privacy settings on the account must be set appropriately for the purpose of the work.

22. Adults who work with children or young people in a professional or volunteer capacity should also take care with their own posts, privacy settings and who they accept as friends. Further advice on this is available in the Oldham Council Guidance for Council Employees Safer Use of Electronic Media and in the advice and guidance published by trades unions and professional bodies.

23. In risk-assessing use of social networking, the specific nature of the social networking site under consideration needs to be taken into account. Facebook and Twitter, for example, reveal very different amounts of personal data; many of the risks commonly associated with the former would not apply to the latter. A social network controlled professionally (such as may be set up with Ning, for example) will work very differently to one controlled by a corporation such as Facebook. These general guidelines and the need to consider safety would apply in all circumstances however.

24. Children and young people should receive advice and education about the safer use of social networking. This should include the ethics of young people's online citizenship (the 'rights' and 'wrongs' of behaviour online) as well as the details of risks associated with social networking and the techniques for minimising those risks.

25. Many of the best-known social networks have a minimum age of 13 within their Terms and Conditions, based on current legistation in the USA. Although this does not have legal force in this country, care should be taken in undertaking this safety education with children below this minimum age. Whilst teaching the details of Facebook privacy settings (along with the standards of behaviour expected online) is a valuable safeguarding measure, care must be taken not to undermine parents/carers resisting underage use. It can be highly effective to allow children to log in to their own Facebook accounts, for example, in a guided activity checking and amending privacy settings, examining how the targeted advertisements on the account indicate the extent to which Facebook is tracking them, exploring the terms and conditions, etc… but staff should avoid unintentionally giving the impression that the agencies (including school) endorses or approves of underage use. As an example, the following would apply as a guide where children under 13 are allowed to log in to Facebook for esafety education within a school:

    - The session should include focus on standards of behaviour online as well as safety and privacy settings, with the aim of creating peer pressure against unpleasant behaviour.
    - A letter should be sent to parents explaining the school's stance as well as alerting parents to the age limit and the risks.
    - An offer should be made to parents of further information to enable them to keep their children safe online.
    - The information provided to children and parents/carers should include how to deactivate as Facebook account as well as how to control privacy.

Further advice on this is available from the City Learning Centre which runs workshops on this model for children in schools and other settings.

Mobile Devices

26. An increasing amount of online activity now takes place via mobile devices rather than fixed or 'luggable' computers (laptops).

27. Whilst this development brings enormous value to the user, and particularly to educational settings, it also brings specific challenges and dangers that young people and the professionals who work with them should understand and know how to handle:

    - Mobile devices are more likely to be stolen, potentially giving the thief access to personal data and online accounts from email and social networking through to banking and online shopping.
    - Theft or 'borrowing' of an unprotected device enables it to be misused to send messages appearing to be from the owner (as a prank or a form of bullying).
    - Many apps on mobile devices report by default the user's location (to their contacts on social networking sites, for example). Some apps (and portable gaming machines) also tell each other of other users in the vicinity.
    - Many mobile social networking apps (such as Facebook) provide the user with only limited access to privacy and other settings, requiring the user to use a traditional desktop computer to fully set up the privacy controls they need on the mobile device.
    - Many mobile social networking apps (such as Facebook) will by default access other data (such as contacts) on the mobile device potentially sharing this data with a wide circle of others.
    - The ease of use of the camera and video camera in mobile devices means that images and video can be posted online in seconds, and are then un-retrievable.
    - Services popular with young people (such as Blackberry Messaging) are often not used and therefore not well-understood by their parents or other adults who work with them.

28. All professionals working with young people who use personal mobile devices should ensure that they have an appropriate pass code set to prevent access by anyone who has taken the device. Similarly, passwords for email and other online services should not be saved on the device.

29. Mobile devices should not be used to store children's personal data (and nor should laptops). It is perfectly reasonable and normal for teachers, for example, to have spreadsheets of assessment data, targets, etc that they use for monitoring and analysis but not personal data (such as home addresses, contact telephone numbers, medical information, photographs etc) which should never be needed on such a device.

30. Particular care should be taken on field trips, for example, where the following would apply:

    - Where such a trip is during school time, consideration should be given to whether it is safer for the trip leader to contact the school for a member of staff there to look up these details and make and receive any necessary emergency calls, rather than the person out on the trip doing it
    - In general, remote access to their MIS via the web should be used rather than electronic data on a portable device, with hard copy taken on the trip as back-up.

31. It is for each school or setting to determine its own approach to the management of young people's own mobile devices, but where they are allowed it is essential that the rules and ethics of their use are both

promoted and taught, including such issues an not photographing people without their permission, taking care of personal security, etc. (It is effective to undertake this through 'pupil voice' or similar activity).

32. All provisions of this policy and advice should be applied to mobile devices just as with fixed devices.

Images, Video and Video Conferencing

33. All young people's settings should be cautious about use of images of young people on their websites or other publicity. In general,

    - Images should not be accompanied by personal data identifying the young person.
    - Appropriate parental/carer permission should be gained, or the images not used.
    - Additional care should be taken with images of young people in vulnerable circumstances, where - even if permission is given - the setting still has responsibility to ensure that its use does not compromise the safety of the child or any other person. (Consider the example of a child whose parent is fleeing domestic abuse, for example).

34. All young people's settings should also be cautious with images of young people stored on computers in their establishments, considering the possibility that another young person may access and publish such images (or altered versions of the images). All settings are responsible for the security of any young person's data they hold, including images.

35. Staff should also be aware that photographs taken for print purposes may end up also online (e.g. local newspaper articles being published also in online editions).

36. This guidance around images applies also to moving images – i.e. video and video links. Care should be taken with the security of video files on computers, servers, and portable drives, as well as those remaining on a video camera after use. Any copies unsecured (e.g. on the video camera itself) should be deleted.

37. Use of technologies such as Skype, Facetime, or 'old-style' video-conferencing should be undertaken within these same guidelines. In particular, children should not give out personal information over any video link, and the school or other setting providing the link should ensure they know who is on the other end. (Cameras should not be focused on children until the link with the intended participant is established and confirmed).

38. Children and young people should be taught safety guidelines and citizenship ethics around production of images and video for web-publication. The resources produced by the BBC for BBC News School Report are useful for this - further advice is available from the City Learning Centre.

'Sexting' - self-generated explicit images of children or young people

39. There have been an increasing number of incidents where young people have shared sexual images of themselves ('sexting'). Where this happens, images have usually been shared with a partner or intended partner as a form of flirtation or - in the eyes of the young person - 'safe sex'. Someimes this is as a result of pressure, however.

40. What ever had promopted the sending of the image, the act itself poses a risk to the young person in the image: once it has been shared it is liable to be be distributed further. The young person is then exposed to risk of high-level bullying and to the possibility of being stalked by a paedophile who has become fixated on them after finding the image online.

41. This action may also place both the sender and the recipient in a position of having committed an offence under the Protection of Children Act 1978 (See Appendix Four).

42. Young people of an age likely to consider such actions should be educated about the risks; there are useful video resources available for this (contact the City Learning Centre for details).

43. Any incidents that come to light should be handled carefully bearing in mind both that possession of the images may constitute an offence in itself, and that the child or young person whose image has been shared is at risk and may already be subject to an exploitative relationship. All incidents should be dealt with as in the Sample Procedure in Appendix Three (page 12).

44. There have been a number of cases of images or video of children or young people under the age of 16 engaging in sexual activity being shared. These are legally images of child sexual abuse, even if they have been shared by others of the same age. All such cases are evidence of a child or young person being sexually exploited and should be dealt with as such - see the Sample Procedure in Appendix Three (page 12).

Preventing Violent Extremism

46. If not used with appropriate critical awareness, web-based information and social networking can increase the risk to a young person of being drawn into violent extremism. Any such cases should be dealt with in accordance with the LSCB's Preventing Violent Extremism policy.

eSafety Training

47 The Oldham Local Safeguarding Children Board (LSCB) arranges training for multi-agency audiences and quality assures training for single agency settings (eg schools). Settings should ensure that *all staff* have received this training (including new staff) and that it is periodically renewed - technology and young people's use of it both undergo rapid change.

Reviewing Policies

48. All young people's settings schould have esafety comprehensively covered within their policies. This policy and guidelines document should be used to review these policies.

49. In some settings a full e-Safety Policy will be the best approach, in others a shorter policy that cross-references where esafety appears in other policies will be more appropriate. *In no cases should esafety be addressed solely as an aspect of ICT.*

50. Specific reference to esafety would be expected in the following policies (this is not an exhaustive list):

- Safeguarding
- Child Protection
- Anti-Bullying
- Curriculum
- Educational Visits / Offsite Trips

Monitoring and Review of this Policy and Guidance

51. Use of this policy and guidance will be monitored through a sampling excercise in 2013. It will be formally reviewed in 2014.

Appendix One:

Useful websites.

CEOP	www.ceop.gov.uk/
Think U Know	www.thinkuknow.co.uk
Childnet	www.childnet-int.org
Internet Watch Foundation	www.iwf.org.uk
eSafety Week	www.esafetyweek.info
Oldham eSfety on Facebook	www.facebook.com/oldhamesafety

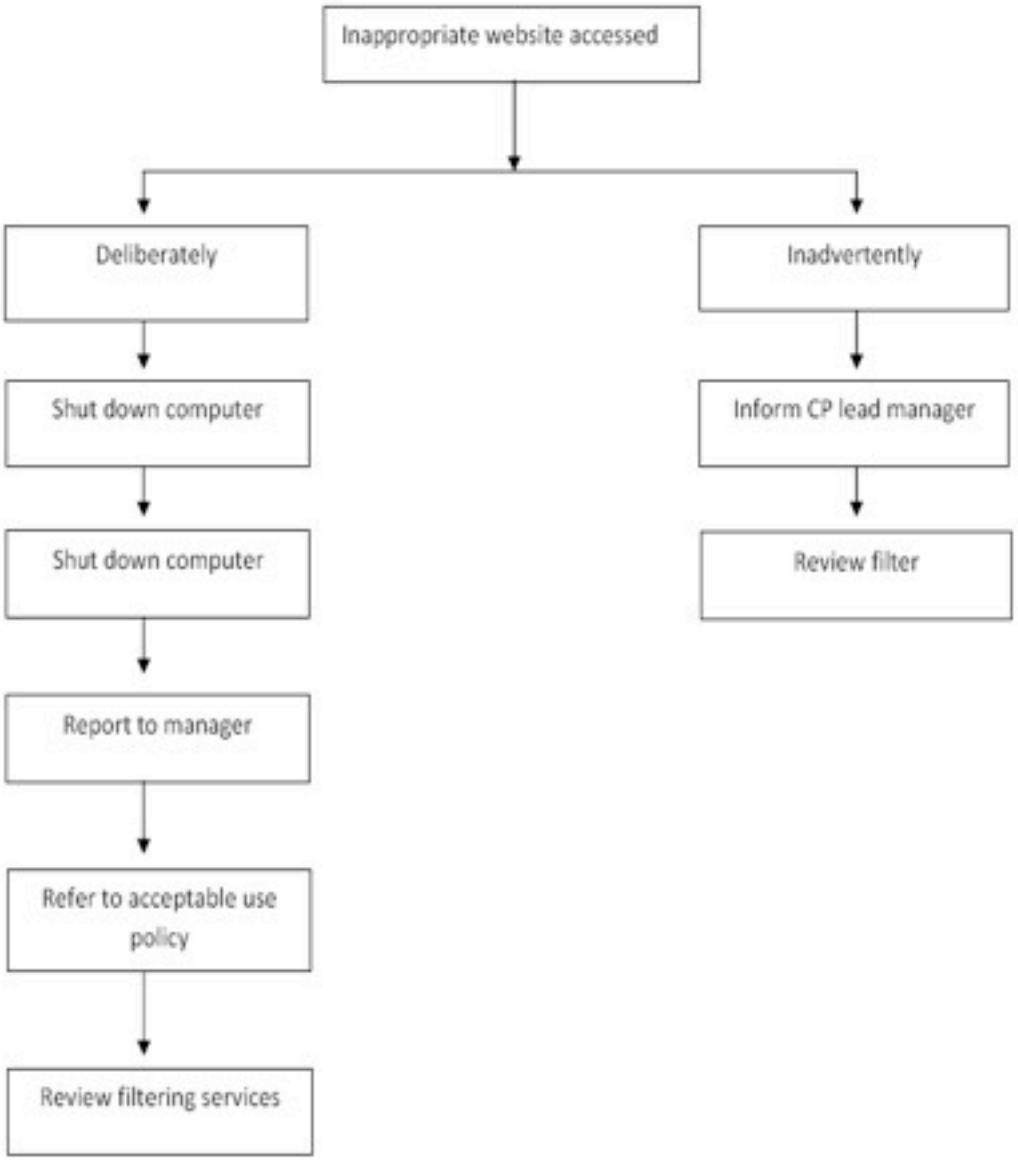
Appendix Two:

Sample Procedure (to be incorporated into existing procedures)

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

1. 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.
2. 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 child protection 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.
    - Decide on appropriate sanction (if young person)
    - Notify parent/carer
3. 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.



4. An illegal website is accessed or illegal material is found on a computer.
5. The following incidents must be reported directly to the police (0161 872 5050):
    - 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.
- Harassment

6. 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 / 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), ceop.police.uk/.
    - 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. 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 .
- Report to the Local Authority Designated Officer (0161 770 8870)
- Preserve the information received by the child if possible.
- Contact the police as necessary.

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 Child Protection Leader so that new risks can be identified.
    - Contact the police or CEOP if appropriate.
9. Where staff or adults are posted on inappropriate websites or have inappropriate information about them posted this should be reported to the manager.
10. 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.

Appendix Three:

Sample Procedures for dealing with 'Sexting'

If images or video of children engaged in sexual activity or in revealing poses are known to have been posted online the following guidelines should be followed:

- If the images are on a computer follow the guidelines in 7.5. Where the existence of the video or images has come to attention through young people talking about them or viewing them on their phones the following measures should be taken:
- Police should be contacted immediately and a CEOP report made giving the available information. The police will be in a position to make judgements about how matters are pursued in relation to offences and offenders.
- The nominated person for child protection should initiate a CAF. Through the CAF process judgements will be made about the best means of supporting the child.

- Sites or networks on which the images should be alerted to the existence of illegal material. It is important that material online be removed as soon as possible, but staff must not put themselves at risk of illegality. Once the matter has been reported to the police their advice on this must be followed.

- Any young people who have themselves posted potentially illegal material should be told to remove the items, and warned that police action may follow if they do not. Through the CAF process parents may also be involved.

- In some cases there may not be an obvious means of flagging or reporting the image (for example where a revealing picture of a young person has been used in an another young person's Blackberry Messaging profile). Even in these circumstances the existence of the image should be notified to the network provider (eg RIM for a Blackberry) and police action may be necessary to ensure its removal or eengage the co-operation of the young person who has control of the image.

- The incident should be logged through the organisation's own monitoring / line management procedures.

- Appropriate educational/pastoral work should be undertaken with all young people involved.

Appendix Four:

Acceptable Use Policies

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.

2. Example 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 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.

Appendix Four:

Legal framework

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

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:

1. **The Sexual Offences Act 2003**

    - 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.
    - 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.
    - It is also an offence for a person in a position of trust to engage in sexual activity with 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).
    - Any sexual intercourse with a child under the age of 13 commits the offence of rape.

    More information about the 2003 Act can be found at www.teachernet.gov.uk

2. **Communications Act 2003 (section 127)**

    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.

    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.

3. **Data Protection Act 1998**

    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.

4. **The Computer Misuse Act 1990 (sections 1 – 3)**

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

- 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).

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

5. **Malicious Communications Act 1988 (section 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.

6. **Copyright, Design and Patents Act 1988**

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

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.

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.

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

7. **Public Order Act 1986 (sections 17 – 29)**

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.

8. **Protection of Children Act 1978 (Section 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 a 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.

9. **Obscene Publications Act 1959 and 1964**

Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

10. **Protection from Harassment Act 1997**

- 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.

- 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**

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.

12. **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. Covert monitoring without informing users that surveillance is taking place risks breaching **data protection** and privacy legislation.