Lambeth Safeguarding Children's Board

e–Safety Strategy & Policy

Document Control
Version: V5

Approved By: Lambeth Safeguarding Children's Board 26 September 2011

Effective From: 01 October 2011

Author: Roddy Leith

Page No

1. The Lambeth Safeguarding Children's Board 3

2. Introduction and Scope 4

3. Issues and Challenges to the LSCB 5

4. Strategic Direction 6

5. Strategic Priorities 6

6. The Legal Framework 10

7. Glossary of Terms 10

1. Introduction

The Lambeth Safeguarding Children's Board (LSCB), is the key statutory body which has lead strategic responsibility for improving the way in which children and young people are safeguarded in Lambeth and for quality assuring the effectiveness of all its partner agencies.

This strategy document is the Lambeth Safeguarding Children Board's response to the challenges posed by the increasing use of digital technologies used by children and young people.

The LSCB recognises e-safety issues and the potential dangers and risks these can pose to children and young people. We believe that structured planning and intervention will help to ensure appropriate, effective and safer electronic forms of communications for our children and young people. Appropriate guidance for parents / carers, foster carers, schools, partner agencies and voluntary organisations will enable effective e-safety practices, policies and procedures.

All agencies providing services to children have a duty to understand e-safety issues as part of its wider safeguarding duties; recognising their role in helping children to remain safe online while also supporting the adults who care for children. However the LSCB acknowledges that its role is strategic rather than operational as it is for partner agencies to develop and embed their own operational policies and procedures, and lines of accountability, in safeguarding children when using Internet, Digital and Mobile Technologies (IDMT) It is envisaged, however, that this strategy, and suggested policy, will provide a framework for partner agencies in this regard in line with the following definition of e-safety and LSCB vision.

Definition of e-safety
The term e-safety is defined for the purposes of this document as the process of limiting the risks to children and young people when using Internet, Digital and Mobile Technologies (IDMTs) through a combined approach to policies and procedures, infrastructures and education, including training, underpinned by standards and inspection *(source BECTA. BECTA was closed by the coalition government 31st March 2011).*

LSCB Vision

Our vision is that all children and young people, all parents/carers and foster carers and all those working with children and young people recognise the risks and potential dangers that may arise from the use of Internet Digital and Mobile Technologies, that they understand how to mitigate these risks and potential dangers and are able to recognise, challenge and respond appropriately to any e-safety concerns so that children and young people are kept safe.

The LSCB is aware that the understanding and use of Internet, Digital and Mobile Technology (IDMT) is essential to helping and encouraging every Lambeth child to reach their full potential however it was recognised by the board that a comprehensive but easy to understand e-safety strategy and policy should be available for all organisations to access via the LSCB's independent website www.lambethscb.org.uk .

For this purpose the board established an e-safety subgroup to steer this time bound project in line with the agreed Terms of Reference (see Appendix 3).

The e-safety sub-group meets bi-monthly and is chaired by the Senior Safeguarding Manager for Universal Services within Lambeth Children & Young Peoples Services. Membership includes representatives from Lambeth Children's Safeguarding Team, Schools ICT, Early Years, Libraries, Alternative Education and the Police.

2. Scope

Working Together to Safeguard Children 2010 outlines the relationship the LSCB has with wider arrangements to improve the overall wellbeing (Every Child Matters outcomes) of every child in the Borough. This is in line with the general duty to safeguard and promote the wellbeing of children by; protecting children from maltreatment, preventing the impairment of their health or development, ensuring children grow up in circumstances consistent with the provision of safe and effective care and undertaking that role so as to enable children to have optimum life chances and enter adulthood successfully. *(Source London Child Protection Procedures V4)*

Specifically the ***Stay Safe*** outcome states that children & young people be:

- Safe from maltreatment, neglect, violence and sexual exploitation;
- Safe from accidental injury and death;
- Safe from bullying and discrimination (which includes cyber-bullying)
- Safe from crime and anti-social behaviour in and out of school
- Be secure, stable and cared for.

It is therefore under this outcome that the context for e-safety arises.

Under Section 11 of the Children's Act 2004, all professionals have a duty to safeguard and promote the well being of children and young people. It is therefore universally recognised and accepted that this duty becomes everyone's responsibility. Children & young people can only be safeguarded properly if everyone involved with them works effectively together and accepts responsibility for promoting their welfare and includes adults who are their parents / carers or foster carers as, unfortunately, children and young people may now be abused in their homes, community settings and educational settings by adults, other children or strangers through the advancement of digital technologies.

We (the LSCB) therefore have to raise awareness and educate those involved in a young person's welfare and development about the dangers that young people can face in the online virtual world, whilst accepting that safety in the online virtual world is not a technological issue, that is to say the removal or banning of access to digital technologies is not the answer in itself but rather education and training, for both children and adults, around responsible use and potential dangers.

For many children and young people in Lambeth, the online 'virtual' world is as real to them as the 'real' world; however the digital or online world needs to be seen in the same context as the real world in that it also has dark alleys and dangerous places which children and others would be unwise to venture into. A false sense of security encourages a perception that a young person is safe as they are perhaps in the comfort and relative safety of their own room when the actual dangers are all too real. Therefore through education and support we must encourage and enable children and young people to make safe choices in the digital online world in the same way that we do for children and young people in the 'real' world.

Despite this, digital technologies offer opportunities to learn and develop, communicate, be creative and be entertained in an environment many assume to be safe and therefore, feels 'safer' than the real world outside.

However, we now have a greater understanding to the extent of these day to day dangers this virtual world can pose to children and young people, such as:

- Children and young people have been groomed* online by adults (often pretending to be other young people) with the ultimate aim of exploiting them sexually.
- Children and young people have been bullied by other young people via social networking websites and text messages and other electronic media.
- Inappropriate (i.e. threatening or pornographic) images of children and young people have been uploaded and circulated via social network websites, mobile telephones and video broadcasting websites such as You Tube, often by other young people.
- The dangers attached to gang culture can rapidly accelerate online if threats of violence, threats to an individual's life or threats of retaliation are posted online by opposing gang members.
- Children and young people can readily access inappropriate websites and images online (often in innocence).

(*grooming - A course of conduct enacted by a suspected paedophile, which would give a reasonable person cause for concern that any meeting with a child arising from the conduct would be for unlawful purposes (Sexual Offences Act 2003)).

Ignoring the dangers that children and young people can face would lead to serious gaps in our responsibilities towards safeguarding and child protection therefore partner agencies are requested to refer to the non statutory practice guidance in paragraphs 11.93 to 11.97 of *Working Together to Safeguard Children 2010.*

3. Issues and Challenges to the LSCB

We have a moral and legal responsibility to meet the Every Child Matters agenda and ensure that our community is committed to its responsibility towards e-safety.

Due to the rapid advancement of digital technologies, children and young people embrace and understand advancement in the internet and mobile technologies as the 'norm' and view this 'virtual world' as an extension to their physical world – in this sense children are often referred to as 'digital natives' However children / young people often do not understand that their online behaviour may have offline consequences.

Common technologies used include:

- The Internet
- Email
- Instant Messaging
- Blogs / Twitter
- Podcasts
- Social Networking Sites such as Facebook
- Location based social networking such as Google Latitude
- Video broadcasting sites such as YouTube
- Chat rooms – although diminishing in popularity
- Online gaming rooms and platforms
- Music download sites
- Mobile phones with camera and video functionality
- Applications

Very often, children and young people's methods of communication and emotions are

relayed to others via digital technology whereas for adults, IDMT is viewed as a tool, solely to be used for a specific task (e.g. being accessible to others, using the internet etc). Adults may not necessarily understand the apparent necessity for children and young people to constantly be online but should appreciate that excessive usage of IDMT could impair a child's welfare or development by inhibiting real life social relationships and should, therefore, have some degree of control over the amount of time young people have access to IDMT.

Parents and carers may also view this seemingly constant use of IDMT as a barrier to communication rather than an aid and we can therefore no longer consider the wellbeing of children and young people and safeguard them without addressing the potential dangers of the online world.

4. Strategic Direction

The LSCB e-safety subgroup will develop and implement this strategy and policy within the council and its member agencies and encourage other partner agencies to adopt this approach. This strategy and policy will be accessible via the LSCB's website www.lambethscb.org.uk .

The e-safety subgroup will also monitor, evaluate and review updates and advancements in digital technology which may impact on e-safety issues and provide a best practice framework by:

- Being a central point of contact for advice, guidance and networking.
- Identifying & co-ordinating local e-safety champions (or leads).
- Liaising with the LSCB Training subgroup and develop multi-agency training and briefing sessions as required for partner agencies, the voluntary sector, schools and other educational establishments.
- Promoting e-Safety within the wider local community.
- Encouraging agencies to incorporate and embed e-safety into their existing safeguarding and child protection procedures enabling them to recognise and identify e-safety concerns and ensure these are escalated and resolved via the correct platforms (see Appendix 5).
- Liaising with and participating in research with agencies such as the National Education Network (NEN) Safeguarding Group for updates on best practice in e-safety.
- Publish relevant research and statistics on the LSCB website, as and when identified.
- Publishing information gained through the datasets from partner agencies.

The LSCB also identified and agreed three key areas of concern it wanted a particular focus on. These were:

1. Looked after children
2. Parents and carers
3. Cyber bullying

For this purpose, the e-safety subgroup will develop additional specific guidance on key areas of concern after consultation with children and young people, their parents / carers and foster carers by way of appendices attached to the policy.

5. Strategic Priorities

The LSCB e-safety subgroup subsequently agreed six key strategic priorities in order to achieve this aim.

Each priority is supported by a variety of objectives which must be met.

5.1 Raise awareness and understanding of the e-safety issues children and young people face when accessing IDMT.

We will:

- Enable all schools and educational settings to tackle e-safety issues by embedding a local e-safety strategy and policy into their programme and daily practice.
- Make e-safety a talking point for young people, especially around offline consequences of online behaviour.
- Ensure young people understand the barriers that must be in place to protect them from abuse or exploitation from the professionals that work with them (i.e. the potential dangers young people may face when they send 'friend requests' or give their phone numbers to professionals etc).
- Enable young people to understand the dangers posed by those that may want to exploit them online – either by sexual grooming or by phishing* for personal details, especially financial details.
- Ensure children with additional vulnerabilities (i.e. is disabled, have learning difficulties or are out of mainstream education etc) are provided with guidance appropriate to their level of understanding.
- Ensure that looked after children are provided with age appropriate guidance in relation to e-safety.
- Promote the dangers of cyber bullying and ensure all young people understand what can constitute cyber bullying and the severely damaging effects this can have, especially in light of the real 'life and limb' physical risks of harm that may ensue or escalate from instances of cyber-bullying – as high profile cases have shown.
- Ensure young people understand that the taking of and distribution of indecent images of children is a criminal offence under s45 of the Sexual Offences Act 2003.
- Encourage young people to take advantage of online resources which help to safeguard them.
- Ensure young people know how to recognise, challenge and respond to e-safety issues.

(*phishing – a scam by which an individual is duped into revealing personal and confidential information about themselves which the scammer can use illegally – usually by phone, email or text message).

5.2 Raise awareness and understanding of e-safety issues children and young people face to parents/carers and foster carers and ways to mitigate these risks.

We will:

- Improve levels of awareness and understanding amongst parents/carers and foster carers of the risks posed to children & young people by their use of the Internet, Digital and Mobile Technology (IDMT) and how to minimise and mitigate this.

- Promote the dangers and signs and symptoms of cyber bullying to parents/carers and foster carers, highlighting the very real physical risks of 'life and limb' harm that may escalate out of instances of cyber-bullying – as high profile cases have shown.
- Improve awareness amongst parents/carers and foster carers of available e-safety resources including those available online.
- Increase awareness of the protocols in responding to and reporting e-safety incidents to local and national agencies including the local authority safeguarding representative / social care and CEOP (Child Exploitation & Online Protection Centre – www.ceop.police.uk) / the Police. (see Appendix 5).

5.3 Raise awareness and understanding of e-safety issues amongst all agencies and organisations within Lambeth including schools.

We will:

- Ensure the LSCB has representation from key member agencies and is provided with regular updates and briefings from the e-safety subgroup.
- Incorporate e-safety into existing multi-agency training for key members and partner agencies and continue to raise the profile of e-safety amongst professionals.
- Ensure partner agencies have an e-safety training strategy.
- Obtain commitment to the e-safety agenda at executive level from our key partner agencies.
- Encourage schools and other agencies to take advantage of available e-safety resources (including online) and to incorporate and embed e-safety principles into their curriculum.
- Encourage schools and other agencies to have local e-safety 'champions'.

5.4 Enable partner agencies and local organisations to identify potential risks that young people may be exposed to by their increasing usage and reliance on IDMT and appropriately respond to any incidents of concern.

We will:

- Encourage partner agencies to adopt and incorporate the principles of this strategy and policy into their existing policies and procedures (i.e. Acceptable use of Internet, Staff Code of Conduct etc) which should:
    - enhance their existing responsibilities for educating and safeguarding children,
    - improve local protocols for responding to, reporting and investigating e-safety incidents,
    - help minimise the risk of allegations being made about members of staff.
- Ensure all staff working with young people are aware of their professional boundaries when communicating with young people.
- Ensure agencies are familiar with and understand the protocols in responding to and reporting e-safety incidents and concerns including the local authority safeguarding representative / social care and CEOP (Child Exploitation & Online Protection Centre – www.ceop.police.uk) / Police.
- Enable a rapid multi-agency response to e-safety incidents.

- Ensure that all e-safety incidents are recognised, reported and investigated as appropriate (see Appendix 5). This includes the taking of and distribution of indecent images of children which should always initiate a referral to Social Care for both victim and perpetrator(s) where these are children or young people and notification to the Police where perpetrators are adults.

5.5 Encourage safe access to IDMT to all children and young people.

We will:

- Obtain an overview of general internet access within the community including schools & educational settings, youth sites, libraries and home settings including mobile phones.
- Encourage safe access to IDMT by promoting the usage of age appropriate filtering systems to children & young people:
    - in the home (including care home) environment or foster care placement and to those with parental control,
    - by mobile phone – those with parental consent should limit their children's internet access by utilising the mobile phones settings,
    - in schools and educational settings and environments such as youth clubs, community groups, libraries and hospital settings,
    - in commercial access points such as internet cafes (where possible).

5.6 Monitor e-safety arrangements and incidents in Lambeth and the impact of this strategy.

We will:

- In monitoring the effectiveness of this strategy; gather as accurate as possible, an up to date profile of e-safety arrangements with all LSCB partners, including;
    - The number of partner agencies with acceptable use policies in place,
    - The number of partner agencies with an identified e-safety lead,
    - The number of partner agencies using accredited internet service providers,
    - The number of partner agencies with a filtering and monitoring plan in place,
    - The number of partner agencies with an e-safety awareness and training plan in place.
- Gather qualitative information on young people's personal views and concerns about e-safety and common risks i.e. cyber bullying, chatroom dangers, social networking sites etc and trends.
- Seek to ensure partner agencies monitor the following as a suggested minimum dataset of e-safety incidents:
    - A description of the e-safety incident,
    - Who was involved,
    - How the incident was identified,
    - What actions were taken and by whom,
    - Conclusions of the incident.
- Review and monitor all IDMT related safeguarding incidents and trends, including the overall nature and range of IDMT related safeguarding incidents from partner agencies and report to LSCB, specifically considering;
    - Why the incident happened,

- Any preventative measures,
- Effectiveness of the response by the agency,
- Lessons learnt – to inform ongoing policy and practice.

6. The Legal Framework:

- Racial & Religious Hatred Act 2006
- Sexual Offences Act 2003
- Police & Justice Act 2006
- Computer Misuse Act 1990 (s1-3)
- Communications Act 2003 (s127)
- Data Protection Act 1998
- Malicious Communications Act 1988 (s1)
- Copyright, Design & Patents Act 1988
- Public Order Act 1986 (s17-29)
- Protection of Children Act 1978 (s1)
- Obscene Publications Act 1959 & 1964
- Protection from Harassment Act 1997
- Regulatory of Investigatory Powers Act 2000

8. Glossary of Terms

- LSCB – Lambeth Safeguarding Children's Board
- IDMT – Internet Digital & Mobile Technology
- ICT - Information & Communication Technology
- NEN - National Education Network
- CEOP – Child Exploitation and Online Protection Centre (part of National Crime Agency)
- BECTA - British Educational Communications & Technical Agency (now closed)

London Borough of Lambeth e–safety Policy

Page No

1	Introduction	13
1.1	Definition of Safeguarding and e-safety	13
1.2	LSCB Vision	13
2.	Background	13
2.1	Scope	14
3.	Aim of Policy	15
4.	Principal Responsibilities	15
4.1	Education and Learning	16
4.2	Keeping up to date with technology	17
4.3	Managing Information & Communications Technologies (ICT)	17
4.4	Filtering	17
4.5	Email	18
4.6	Mobile Phones	19
4.7	Social Networking	19
4.8	Web Cameras	20
4.9	Gaming	21
4.10	Cyber Bullying	21
4.11	Publishing Young People's images and work	22
4.12	Illegal Downloading	23
5.	Date Protection	23
6.	e-Safety Complaints	23
7.	Internet in the local community	24
8.	Monitoring e-safety & Reporting Abuse	24
9.	Promoting the Policy	25
10.	Staff Engagement	25
11.	Engaging with Parents / Carers and Foster Carers	26
12.	Additional Online Advice & Support	26
	Appendix 1 – e-Safety Advice to Parents / Carers and Foster Carers	28
	Appendix 2 – Cyber Bullying	32
	Appendix 3 – Terms of Reference	34
	Appendix 4 – Safer Working Practices	35
	Appendix 5 – Procedure for managing e-safety concerns	37

Policy

1. Introduction

This safeguarding policy and guidance has been developed by the Lambeth Safeguarding Children's Board (LSCB) e-safety subgroup and is suitable to be adopted as a model of best practice by all stakeholders, partner agencies, schools and educational settings and all other organisations within the community in order to safeguard children and young people from the potential dangers in the online world.

It can also be used as a point of reference for children and young people and their parents/carers, foster carers and those in a position of trust with young people.

1.1 Definition of Safeguarding

The following is the accepted definition of 'Safeguarding and the Promotion of Wellbeing for children;

- To protect children from maltreatment,
- To prevent the impairment of a child's health or development,
- To ensure the child grows up in circumstances consistent with the provision of safe and effective care, and,
- To ensure that this role is undertaken so as to enable children to have optimum life chances and enter adulthood successfully.

1.2 Definition of e-safety

In addition to the definition set out at 1.1 the term e-safety is specifically defined for the purposes of this document as the process of limiting the risks to children and young people when using Internet, Digital and Mobile Technology (IDMTs) through a combined approach to policies and procedures, infrastructures and education, including training, underpinned by standards and inspection *(source BECTA. BECTA was closed by the coalition government 31st March 2011)*.

1.3 LSCB Vision

Our vision is that all children and young people, all parents/carers and foster carers and all those working with children and young people recognise these risks and potential dangers that may arise from the use of Internet, Digital and Mobile Technologies, that they understand how to mitigate these risks and potential dangers and are able to recognise, challenge and respond appropriately to any e-safety concerns so that children and young people are kept safe.

2. Background

Under Section 11 of the Children's Act 2004, all professionals have a duty to safeguard and promote the welfare of children and young people. It is therefore universally recognised and accepted that this duty becomes everyone's responsibility. Children and young people can only be safeguarded properly if everyone involved with them works effectively together and accepts responsibility for promoting their welfare and includes adults who are their parents/carers and foster carers.

Working Together to Safeguard Children 2010 outlines the relationship the LSCB has with wider arrangements to improve the overall wellbeing (Every Child Matters outcomes) of every child in the borough.

Specifically the ***Stay Safe*** outcome states that children & young people be:

- Safe from maltreatment, neglect, violence and sexual exploitation,
- Safe from accidental injury and death,
- Safe from bullying and discrimination (which includes cyber bullying),
- Safe from crime and anti-social behaviour in and out of school,
- Be secure, stable and cared for.

It is therefore under this outcome that the context for e-safety arises.

2.1 Scope

The LSCB therefore has to raise awareness and educate those involved in a young person's welfare and development about the dangers that young people can face in the digital world, whilst accepting that safety in the digital world is not simply a technological issue, removal or banning of access to digital technologies is not the answer but rather education around responsible use and potential dangers is the key.

Unfortunately, children and young people can now be abused in their homes, community settings, and educational settings through the use of digital technology by adults, other children or strangers. We therefore have to raise awareness and educate those involved in a child's / young person's welfare and development about the dangers that children/young people can face in the online world.

For many children / young people in Lambeth, the online 'virtual' world is as real to them as the 'real' world; however the digital world needs to be seen in the same context as the real world in that it also has dark alleys and dangerous places which children and others would be unwise to venture into. Children / young people do not always recognise the inherent dangers of the internet and often do not understand that online behavior may have offline consequences.

Despite this, digital technologies can offer children and young people opportunities to learn and develop, communicate, be creative and be entertained. The advantages of the internet can and should out weigh the disadvantages.

However, we now have a greater understanding to the extent of these day to day dangers the virtual world can pose to children / young people:

- Children / young people have been 'groomed' online by adults (often pretending to be other young people) with the ultimate aim of exploiting them sexually.
- Children / young people have been bullied by other young people via social networking sites, websites, instant messaging and text messages; this is often known as 'cyber-bullying'.
- Inappropriate (i.e. threatening, indecent or pornographic) images of children and young people have been taken, uploaded and circulated via social network websites, mobile telephones and video broadcasting websites such as You Tube, often by other young people. This is a criminal offence under s45 of the Sexual Offences Act 2003.
- The dangers attached to gang culture can rapidly accelerate online as many gangs 'advertise' or promotes themselves via websites or social networking sites or if threats of violence, threats to an individuals life or threats of retaliation are posted online by opposing gang members.
- Unsuitable websites and images can easily be accessed online.

Ignoring the dangers that children / young people can face would lead to serious gaps in our responsibilities towards safeguarding and child protection therefore partner agencies are requested to refer to the non statutory practice guidance in paragraphs 11.93 to 11.97 of

Working Together to Safeguard Children 2010.

3. Aims

The council has a moral and legal responsibility to meet the Every Child Matters agenda and ensure that our community is committed to its responsibility towards e-safety thus ensuring the safety of children in Lambeth as far as it is practicable to do so.

Due to the rapid advancement of digital technologies, young people embrace and understand advancement in the internet and mobile telephones as the 'norm' and view this 'virtual world' as an extension to their physical world – in this sense children are often referred to as 'digital natives'.

Common technologies include:

- The Internet
- Email
- Instant messaging
- Blogs / Twitter
- Podcasts
- Social networking sites such as Facebook
- Location based social networking such as Google Latitude
- Video broadcasting sites such as YouTube
- Chat rooms, where still used
- Skype
- Online gaming rooms and platforms
- Music download sites
- Mobile phones with camera and video functionality
- Applications

Very often, children / young people's methods of communication and emotions are relayed to others via digital technology where as for adults, IDMT is often viewed simply as a tool, solely to be used for a specific task (e.g. by being accessible to others or to use the internet etc). Adults may not necessarily understand the apparent necessity for children / young people to constantly be online but should appreciate that excessive usage of IDMT could impair a child's welfare or development by inhibiting real life experiences and social relationships and parents and carers should, therefore, have some degree of control over the amount of time children / young people have access to IDMT.

Parents and carers may also view this seemingly constant use of IDMT as a barrier to communication rather than an aid and we can therefore no longer consider the wellbeing of children / young people and safeguard them without addressing the potential dangers of the online world.

This policy therefore recognises the potential dangers and risks children and young people can encounter in the online world and provides advice on how to minimise any potential risk to children and young people.

4. Principals & Responsibilities

This generic e-safety policy should be cross-referenced with local safeguarding policies as well as other policies including Codes of Conduct, Acceptable IDMT/ICT Usage, Anti Bullying and/or Behaviour and Disciplinary policies etc.

The council and its key partner organisations should have designated local **e-safety champions** or be aware of the relevant person / team to contact and report to should they have any safeguarding concerns in line with the procedural flowchart in **Appendix 5** of this policy. It is acceptable for this to be the designated safeguarding lead within each organisation and it is recommended that e-safety champions and safeguarding leads have completed the 'Ambassador' training course administered by the Child Exploitation and Online Protection Centre (CEOP) www.ceop.police.uk .

Organisations must record and monitor e-safety incidents as set out in the LSCB strategy and keep up to date with the emergence of new technologies and trends, including those relating to emailing and mobile phones and be confident in developing appropriate in-house management and communication strategies.

4.1 Education and Learning

The rapid development in IDMT is an essential component in 21st century life for education, leisure, business and social interaction.

Organisations providing internet access to children / young people (schools, libraries, youth clubs etc) must ensure that they do so in a way that is safe and age appropriate for children / young people by way of appropriate filtering systems etc. The consent of the parent/carer or foster carer should always be provided prior to internet access being granted for young people age 16 or under and the young person must agree to adhere to local e-safety rules and acceptable usage policy.

As IDMT is now part of the statutory school curriculum, schools and further educational settings should ensure that young people are taught what is acceptable use of IDMT and be made aware of the potential dangers (including online grooming), the legal implications and be educated in how to effectively research information from the internet and validate it's accuracy. Young people also use IDMT outside of the school environment and must be encouraged to learn how to evaluate information in order to safeguard themselves from unsuitable and inappropriate websites, particularly if the young person is vulnerable (i.e. those promoting eating disorders, teenage suicide, terrorism and pornography etc).

Schools are recommended to take advantage of the many free training resources and educational toolkits available at the ThinkYouKnow and London Grid for Learning websites www.thinkyouknow.co.uk and http://www.lgfl.net/esafety/Pages/ESafetyHome.aspx. These include advice, posters / leaflets, access to other websites, short films, gaming advice etc and also includes age appropriate key stage information and toolkits which can be incorporated into lesson plans. There are also appropriate resources available for children with disabilities and special educational needs.

Schools should also promote and encourage young people to use online facilities such as Cyber Mentors who provide instant online support to young people being bullied or are troubled by something either online or offline. www.cybermentors.org.uk . Cyber Mentors are young people who are trained to respond to other children / young people in need of help and support online and serious issues can be escalated to trained online councillors. Schools may also consider having a trained on site Cyber Mentor for face to face support and training can be accessed by contacting the above website.

The taking and distribution of indecent images of a child or young person under the age of 18 years is a common issue but is also a criminal offence – this often known as 'Sexting' (and includes self taken indecent images). Whilst the Association of Chief Police Officers (ACPO) suggest that this should be dealt with as a safeguarding issue, young people must be made aware that perpetrators (including those who forward these images) could be prosecuted under s45 of the Sexual Offences Act 2003 for the distribution of child

pornography which may result in them being registered on the Sex Offenders Register if convicted. Young People should be under no doubt that this criminal record could impact future further education and employment prospects by barring them from working in many occupations.

As the quantity and quality of information available from the Internet can also be even more difficult to determine than that sourced from other mediums, children / young people must also be taught that the accuracy of information may not always be correct and true, and importantly that the people they encounter on the Internet may not always be who they say they are.

Researching potentially emotive themes such as the Holocaust, Civil Wars or Religion etc provides children / young people the opportunity to develop strong evaluation skills about the conflicting variety of information held on Internet – some which undoubtedly leads to derogatory or misleading web links which may completely deny or wholly misrepresent these events.

Children / young people should also learn and develop the technical and literacy skills required for them to safely refine their own digital publishing and have respect for and comply with copyright or intellectual property rights.

4.2 Keeping up to date with Technology

Designated e-safety champions and ICT leads should register with websites such as Ofcom -

www.ofcom.org.uk and Mashable - www.mashable.com in order to keep up to date with new digital technologies.

4.3 Managing ICT Systems

Security is a complex matter and queries should always be referred directly to the responsible body relevant to the agency. Employees and service users (including young people) should be aware that abuse of recognised policies and procedures could result in a withdrawal of technology provision and potential legal / disciplinary action being instigated against the perpetrator.

All users should therefore be compliant to an Acceptable Use Policy (AUP) or the AUP of your organisation or school.

Common security issues include, for example:

- Users must not act un-reasonably and be inconsiderate of other service users,
- Users not taking responsibility for their own network use,
- Computer and internet access should have appropriate security and anti-virus protection,
- Users seeking to disable or circumvent security measures – filters, encryption etc,
- Personal and sensitive electronic data taken offsite without being security encrypted and authorised by management,
- Unapproved software being introduced into local networks and not authorised by management.

4.4 Filtering

Levels of internet access and supervision must be age appropriate and suitable for the environment the young people are attending. Filtering systems should be secure but adaptable.

Older children and professionals may sometimes require temporary access to a normally restricted website in order to carry out research for a project or study. Providing this can be justified by management, restrictions may be temporarily removed however access should be monitored.

Access controls (filtering) fall into several overlapping types:

- Blocking strategies prevent access to a list of unsuitable sites. Maintenance of the blocking list is a major task as new sites appear every day,
- A walled garden or "allow list" restricts access to a list of approved sites. Such lists inevitably limit young people's access to a narrow range of information,
- Dynamic filtering examines web page content or email for unsuitable words. Filtering of outgoing information such as web searches is also required,
- Rating systems give each web page a rating for sexual, profane, violent or other unacceptable content. Web browsers can be set to reject these pages,
- Access monitoring records the Internet sites visited by individual users. Attempted access to a site forbidden by the policy will result in a report.

Schools in the London Borough of Lambeth generally use an industry standard system as approved by the London Grid for Learning.

Management should ensure that regular checks are made to ensure that filtering methods selected are age appropriate, effective and reasonable. Access to inappropriate websites should always be reported to management and any material perceived to be illegal must be reported to management who should escalate this to the appropriate agency.

4.5 Email

Email is now an essential means of communication which can also be accessible via most mobile phones.

.A degree of responsibility has to sit with children and young people since as soon as email access is permitted; email is very difficult to control. Restricting both incoming and outgoing email to specific addresses is possible however not always practical as email addresses and websites can easily be changed. LGFL mail used by most schools is scanned and filtered for spam and has a safemail setting.

Email should not automatically be considered private and most organisations reserve the right to monitor email however there has to be a balance between maintaining the safety of children / young people and their rights to privacy, which are covered by legislation.

Email content and tone must also be considered. Due to the impersonal nature of email children and young people may write things or be aggressive or dismissive in tone which may be hurtful to others, even if such content or tone is not intended to be hurtful it may still be considered as cyber-bullying.

The use of common email addresses such as *john.smith@lambeth.gov.uk* should generally be avoided for children / young people as this can identify the young person and their general location and children in schools should use email addresses that don't identify your school e.g. *jsmith6.208@ lgfl.net*. Young people should be encouraged to be creative and non-identifiable from their personal email addresses (e.g. *groovejet246@yahoo.co.uk* etc).

General guidance includes:

- Children / young people should not reveal personal information about themselves or other young people via email nor ever arrange to meet strangers by email without specific permission from an adult in authority and this should always be under supervision and preferably in a public place,
- Where possible, organisations such as schools should consider the use of learning platforms and generic email accounts where students are required to submit coursework rather than by pupil to teacher personal accounts,
- Organisations should always prohibit the forwarding of chain emails,
- Professionals should only communicate with young people by email if this has been agreed in advance with the child / young person, their parent/carer/foster carer and management and via equipment owned by their employer,
- Professionals should never disclose their personal email addresses to children / young people,
- Children / young people should advise an adult if they receive offensive or threatening email.

4.6 Mobile Phone

Most young people now have access to mobile telephones which are generally perceived as essential to their day to day living and communicating and now offer access to the internet, instant messaging, email, social networking, a camera and video facilities. Mobile phones are becoming the most commonly used tool for internet access and social networking for young people.

Mobile phones therefore pose one of the biggest online threats to young people as they allow instant access to all forms of IDMT, but unlike static PC's the mobility of the technology means that the online digital world may be accessed by a child or young person virtually anywhere – and as a consequence without the scrutiny or supervision of their parent or carer. This, therefore, makes the user more readily at risk from cyber bullying, being the victim of inappropriate / indecent images being taken and shared with others, being groomed online or by telephone by a stranger or a professional, being the victim of scamming or phishing or even through being a victim of theft or mugging for the mobile phone by an adult or another young person(s).

Children / young people should only share telephone numbers with those known to them and ensure that electronic records (call, text and email logs) are kept of any bullying or threatening telephone calls, text messages, emails or images received which may need to be used as evidence in any police investigation. Children / young people should be careful about accepting invitations to join location based social networking sites such as GyPSii that allow your location to be identified via GPS enabled phones.

Schools and education settings may wish to restrict the use of mobile phones during school hours. However, in some settings permitting responsible use of the mobile phone in conjunction with a cyber bullying education programme is often a better approach.

Scrutiny of the content of a pupil's mobile phone by a school or an alternative education provision (AEP) is not an automatic right and schools and AEP's must clearly outline in their policies that they have the authority to do so under the Education Inspections Act 2006 and specify the circumstances under which this may happen. It is usual for this to be cited in the school policies.

4.7 Social Networking

The Internet provides ready access to online spaces and social networking sites which allow individuals to publish un-moderated content. Social networking sites such as Facebook, Twitter, Chat Rooms, Online Gaming Platforms and Instant Messaging can connect individuals to groups of people which may be friends in the 'virtual' world but who may have never met each other in the real world. Users can be invited to join groups and leave comments over which there may be limited or no control.

Children / young people should be encouraged to consider the associated risks and dangers related to sending or accepting friend requests and posting personal comments, inappropriate images or videos about themselves or their peers and the subsequent difficulty in removing an inappropriate image or information once published. They should also be advised not to publish detailed private thoughts or emotions which could be considered threatening, intimidating or hurtful to others.

Children / young people should also be encouraged to never give out any personal details or images which may identify themselves, their peers, their siblings / foster siblings, their location or any groups, schools or organisations they attend or associate with. This includes real names, dates of birth, address, phone numbers, e-mail addresses, photographs or videos, school attended, IM and email addresses, including those of friends, family / foster family and peers. This also includes any 'gangs' they may be affiliated with.

Children / young people must be advised about e-security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. They should be encouraged to invite known friends only and deny access to others by making their profiles private and only accept friend requests from those already known to them.

Care should be taken to delete old and unused profiles from websites which are no longer used as these will remain accessible to others. Personal information voluntarily shared by a young person is unlikely to remain the same as the person matures and has a greater understanding of how personal information about them can impact on their later lives (i.e. perspective employers making an online search of their name and sighting inappropriate photographs, videos or content etc).

Professionals working or in a position of trust with children / young people (including volunteers) must also familiarise themselves about the risks and inappropriateness of sharing personal information about themselves via social networking sites with young people. They should be made aware of that any inappropriate material posted could affect their professional status. Professionals should restrict access to their friends and family only and 'friend requests' by a young person should be politely declined by explaining professional boundaries. Professionals should also steer clear of social networking sites that young people are known to frequent.

4.8 Web Cameras

The growing popularity for web cameras now allows young people to converse online with each other face to face. This can be more commonly referred to as 'Skyping'. Although the benefits include being able to see the other person you are conversing with, there are also dangers attached to both viewing and being viewed online by another person. These include:

- Being visibly identifiable to the other person. This can also be if anything in the background helps further identify the child / young person such as a school badge, a certificate with the young persons name on it on a wall, a view from a window etc.
- The child / young person does not have an image of the other person they are

conversing with. A common excuse provided would be that their webcam is broken however this does not allow the young person to see the other person they are conversing with and the other person may not be who they say they are.

- Inappropriate or indecent images may be exchanged and recorded and the child / young person blackmailed into performing further sexual acts online which may then be published by the perpetrator or used to further blackmail the young person into meeting them face to face.
- The child / young person can be persuaded to participate in risky behaviours online which could put themselves at risk (i.e. encouraged to remove clothing or attempt suicide online).
- The child / young person may witness the other person performing an indecent or upsetting act.
- The child / young person can be 'groomed' online and encouraged to meet up with the other person.
- Children / young people have instant access to websites such as ChatRoulette which offer random webcam chat with strangers.

Parents / carers and foster carers should only permit webcam access in a common family area under supervision

4.9 Gaming

Online gaming can be good, competitive fun for children / young people providing users are aware of the following risks:

- It can become incredibly addictive in a very short time. Young people can become so immersed in their online communities that they lose touch with the outside world. Certain games demand users to be online during school times and at night, often without their parent's knowledge. Counselling can normally be arranged via a GP for severe addictions.
- Young people may participate in games designed for adults which expose them to levels of language and violence inappropriate to their age – particularly Role Play Games.
- Parents themselves can become gaming addicts and lose any sense of parental responsibility towards their children.
- Gamers can become abusive towards other young gamers, often subjecting the young person to cyber-bullying if the sites have a chat facility.
- There are some children / young people who engage in risky behavior to obtain cheats or knowledge to progress within a game. Adults with a sexual interest in children will encourage them to engage in inappropriate behaviour for rewards including sexual acts via webcam or sex chat.
- Children / young people need to understand that their online behavior has offline consequences and if another online gamer tries to engage them in a sexual manner, this must be reported to the sites moderator and CEOP immediately.

Parents / carers and foster carers should only permit gaming access in a common family area under supervision

4.10 Cyber-bullying

Cyber-bullying can be defined as "*The use of Information Communication Technology, particularly mobile phones and the internet to deliberately hurt or upset someone*" (DCSF 2007).

Children / young people should find using IDMT as a positive and creative part of their everyday life. Unfortunately, IDMT can also be used negatively to target a specific young person or group. When young people are the target of bullying via comments and threats made on mobile phones, social network sites and internet websites, they can often feel emotionally bruised, frightened and alone, particularly if adults around them do not understand or are aware of this occurring. A previously safe and enjoyable environment for young people's activities can become threatening, harmful and a source of anxiety.

Cyber bullying, unlike 'real world' bullying can happen 24 hours a day, 7 days a week and is often perpetrated in the victims home which is usually assumed as a safe and private haven away from the reach of bullies. The scale and scope of cyber-bullying may be very much greater than other forms of bullying due to the very nature of electronic messaging.

Unlike 'real world' bullying the cyberbully may remain anonymous and may never be in the same space as the person being bullied

A number of high profile cases inform us that cyber-bullying can lead to serious physical harm, either through the victim's thoughts and actions turning to self harm or even suicide or in other cases violence can ensue or escalate after cyber-bullying to the extent where a child or young person may be seriously harmed or even murdered in retaliation. These devastating physical consequences of cyber-bully must never be ignored or minimised.

It should also be noted that professionals, especially teachers and other education staff are particularly vulnerable to 'cyber-bullying' by pupils or even ex-pupils, which may include general insults, threats, harassment, defamation, homophobic or racist remarks or other forms of prejudice based bullying . The effects of cyber bullying by young people on adults are equally distressing and the impact on the victim can be just as profound – Government guidance notes remind us that cyber bullying incidents are upsetting whoever the victim is and whatever age they are. Employers should be alert to the possibility and potential for cyber bullying towards members of staff by young people and appreciate there is no 'one size fits all' or single solution to the problem.

Instances of cyber-bullying must be responded to sensitively and in line with existing anti-bullying policies and procedures in schools. The victim of cyber-bullying must be reassured they have done the right thing in disclosing the bullying and be supported. Please refer to the attached **Appendix 2** for further information on this. This should also be cross referenced with the local anti-bullying policy.

4.11 Publishing young peoples images and work

Many organisations create websites inspired by pieces of work and quotations and statements from young people. Often these can include images or videos of young service users which help promote and make the organisation identifiable to other young people.

Still and moving images and sounds can add liveliness and interest to a publication, particularly when young people are included nevertheless the security of children / young people is paramount and names and identifiable locations of young people should never be linked to their images. (i.e. a child placed in a refuge for domestic violence could be traced back to a school by their school uniform).

Children / young people should also be advised when photographs or video footage of them is being taken and images should never be published without the consent of the young

person, and the written consent of their parent/carer or foster carer.

Although it is fairly simple to upload comments, images and videos on social networking and video broadcasting websites, young people must be encouraged to consider the associated consequential risks and dangers in doing this and the difficulties in removing this content, particularly if the content subsequently becomes the property of the publisher. Inappropriate offensive, pornographic or threatening content can have devastating consequences to individuals and groups (including gangs) and young people should be made aware of the legalities and long term implications of doing this.

4.12 Illegal Downloading

Whilst there are many sites where music, videos and software can be legally downloaded, children and young people must be made aware that they could be breaking the law by downloading copyright protected files or by infringing other intellectual property rights.

The various industries affected by illegal downloading (particularly music) do monitor the internet and can take legal action ranging from fines to suing those who hold parental responsibility. It is recommended that websites are thoroughly researched prior to downloading content for personal use.

5. Data Protection

The increasing variety of electronic data that can now be held on children / young people via various databases could potentially be mishandled, stolen or misused.

The Data Protection Act 1998 gives individuals the right to know what information is held about them and provides a framework to ensure that personal information is handled properly. It promotes openness in the use of personal information. Under the Act, every organisation that processes personal information (personal data) must notify the Information Commissioner's Office, unless they are exempt.

The Data Protection Act 1998 applies to anyone who handles or has access to information concerning individuals. Everyone in the workplace has a legal duty to protect the privacy of information relating to individuals. The Act sets the following standards which must be satisfied when processing personal data (information that will identify a living individual). The Act also gives rights to individuals about what information (subject access rights) is held about them. Data must be:

- Processed fairly and lawfully
- Processed for specified purposes
- Adequate, relevant and not excessive
- Accurate and up-to-date
- Held no longer than is necessary
- Processed in line with individual’s rights
- Kept secure
- Transferred only to other countries with suitable security measures.

For further information, please refer directly to the council’s (or your organisation’s) Data Protection Officer.

6. e–safety complaints

Any complaints about e-safety concerns should be progressed via the Council's (or your organisations) recognised complaints procedure which should be readily accessible to all; however efforts should be made to resolve low level issues internally. These must be recorded locally.

All factors in relation to the complaint must be clearly established in order to have substance.

Complaints about employee's IDMT misuse should be escalated to the most senior manager within the organisation and be managed according to recognised disciplinary and child protection procedures.

Employers must have internal methods of scrutinising IDMT use, in particular, the ability to identify sites accessed. This is particularly important where there is an allegation that illegal or inappropriate websites have been accessed.

Potentially illegal issues must always be referred to the police in the first instance.

7. Internet in the Local Community

As internet access is now readily available in all areas of the community, it is recommended that all organisations within the Borough of Lambeth have a consistent approach towards e-safety and adopt the key principles of this policy for local use so that these are embedded in their everyday work.

There is a fine balance to be achieved in ensuring ready access to information whilst providing satisfactory age appropriate protection for children and young people.

Sensitive handling of cultural aspects is important. For instance filtering software should work across community languages and organisations and IDMT policies may need to be translated to reflect the borough's diversity.

8. Monitoring e safety incidents and reporting abuse

Any form of electronic or digital abuse towards young people should in the first instance be reported to the Child Exploitation Online Protection service www.ceop.police.uk , and also reported to the relevant IDMT lead with the organisation. Any incidents which place a young person in immediate danger should be referred to the local police by calling 999.

It is recommended that the CEOP 'report abuse' tool is downloaded onto all computer browsers. This tool provides instant online access to report any form of online abuse. Young people should also be encouraged to download this tool directly onto their electronic devices, especially applications such as personal Facebook profiles.

The monitoring of e-Safety incidents is crucial for learning lessons and to inform actions. Therefore Lambeth's Safeguarding Children Board (LSCB) seeks to ensure that partner agencies monitor the following as a suggested minimum dataset of e-Safety incidents:

- A description of the e-safety incident
- Who was involved
- How the incident was identified
- What actions were taken and by whom

- Conclusions of the incident

The LSCB will review and monitor IDMT related safeguarding incidents and trends via the e-Safety sub group, including the overall nature and range such incidents from information submitted by partner agencies. A report will be presented to the Main Board meeting specifically considering;

- Why the incident(s) happened
- Any preventative measures
- Effectiveness of the response by the agency
- Lessons learnt – to inform ongoing policy and practice

9. Promoting the Policy

It is recommended that organisations include children and young people in the design and layout of their e-safety policy as their perceptions of risk will vary from age group to age group.

Ideally, posters should be displayed in rooms where computers can be accessed which highlight the policy and reiterate that all network and internet usage will be monitored and appropriate action will be taken if abuse occurs.

This policy should be made readily available to parents / carers and foster carers by way of being included and accessible on the organisations published literature and website.

10. Staff Engagement

All staff with responsibility for young peoples learning via IDMT, must be familiarised with this policy and given opportunities to raise issues and concerns they face in their day to day working responsibilities.

All staff must understand that misuse of IDMT will result in disciplinary action being taken against them in line with the Council's 'Using Systems and Data Policy' and the 'Staff Code of Conduct' and 'Disciplinary Procedure'. Other organisations adopting this policy should have similar procedures

Employees unsure of what constitutes acceptable usage of the internet should always check with management. They should be aware that all internet usage is monitored and can be traced back to each individual user.

Staff must also be aware of what is acceptable in terms of their engagement with children and young people via IDMT means.

Staff (including volunteers) should never disclose or share their personal details (i.e. personal mobile phone numbers, email addresses or social networking profiles etc) or send or accept friend requests on social networking websites with children and young people / service users.

Any necessary contact between a young person and a professional should be made via equipment and contact details provided by the employer (not personal equipment / contact details) and be clearly recorded on a need to communicate basis and with the consent of the parent/carer or foster carer. Alternatively, personal contact details for children / young people should be stored centrally by management and only accessed on a need to know

basis as approved by management.

Organisations should adopt an open culture of vigilance in the workplace and staff must feel confident in identifying and challenging poor and/or risky working practices. For further guidance on Safer Working Practice with Technology, please refer to the supplementary guidance in **Appendix 4**

Ideally, training on acceptable usage and responsible e-safety should be provided during the induction period for all new employees with a specific emphasis on professional boundaries, confidentiality and data protection.

11. Engaging with Parents / Carers & Foster Carers

Parents / carers or those with temporary guardianship for young people have responsibility for their children's access to personal and public computers, mobile phones and gaming platforms.

Most children / young people now have access to the internet by way of a home computer / laptop / tablet PC, gaming platform or mobile phone and those with parental responsibility for young people must ensure that this allows for some degree of supervision and that both young people and their parents / carers or foster carers are educated on the risks attached to the internet.

In particular, children and young people with additional vulnerabilities such as:

- Special educational needs
- Physical / learning disabilities
- Are out of mainstream education
- Have behavioural problems
- Are unable to fully understand the consequences of their actions
- Are young offenders or are affiliated with gangs
- Are travellers with inconsistent access to education
- Have language barriers if English is a second language
- Are in short term accommodation or placements

must be made fully aware of the dangers they face online and should have a greater degree of supervision to minimise any risk to them.

Schools are encouraged to work in partnership with parents / carers & foster carers by way of promoting e-safety on their school's website, newsletters and events such as parent's evenings and raising awareness of the resources available to them including those accessible via the Parents section of the ThinkYouKnow website www.thinkyouknow.co.uk .

Signed parental consent should always be received prior to schools and other organisations that work with young people permitting young people under the age of 16 access to the internet, which will form part of the schools AUP .

Please refer to the attached **Appendix 1** for further information on this.

12. Additional Online Advice & Support

www.lambethscb.org.uk	Lambeth Safeguarding Children's Board

www.ceop.police.uk	Child Exploitation Online Protection Centre for reporting internet abuse
www.thinkyouknow.co.uk	Practical online advice and training resource for children, parents and teachers
www.nen.gov.uk	National Education Network - Online advice and training resource for children, parents and teachers
www.cybermentors.org.uk	Social Networking site for young people which trained young people mentor other young people requiring support
www.clickcleverclicksafe.direct.gov.uk	Internet safety advice from the UK Council for Child Internet Safety
www.facebook.com	Very popular social networking website
www.mashable.com	Provides information on how to keep up with new technology
www.ofcom.org.uk	Provides information on how to keep up with new technology
www.digizen.org/cyberbullying	Department of Education and Childnet advice and guidance on cyber-bullying
http://consumers.ofcom.org.uk/2010/10/parental-controls-help-your-children-manage-their-media	How to help your child manage their internet via parental controls
http://www.lgfl.net/learningresources/curriculum/ict/UsOnline2/Pages/UsOnline2.aspx	Learning tool and training resource recommended by London Grid for Learning

Appendix 1
e-safety advice to parents / carers and foster carers

Those with parental responsibility for children should pay particular attention to the following 'rule of thumb' advice in order to safeguard young people they hold parental (including temporary) responsibility for. Please remember that most children / young people have internet access via their own mobile phones, laptops and tablet computers which can be restricted by using the relevant parental consent controls (foster carers should always verify what restrictions they can impose directly with the young persons allocated social worker) and via certain online gaming platforms such as X Box and Playstation.

Parents / carers and foster carers of children with additional needs or vulnerabilities must appreciate that their children will require additional support around e-safety particularly if their child is:

- Disabled
- Has special educational needs or learning difficulties
- Is looked after and placed in an area unfamiliar to them
- Is out of mainstream education
- Speaks English as a second language (or does not understand English)
- Known to have gang associations
- Has been the victim of bullying or crime or has lived with domestic violence
- Is gay or unsure about their sexuality
- Has emotional or learning difficulties or does not fully understand the impact of their actions
- Has been the victim of bullying
- Has inconsistent access to education (i.e. is a traveller)

Parents / carers and foster carers should take advantage of the many online resources available via the parents section of the ThinkYouKnow website www.thinkyouknow.co.uk

It is also recommended that they download the Child Exploitation Online Protection tool onto all computer browsers www.ceop.police.uk .This tool provides instant online access for reporting any form of online abuse.

They should also encourage children to download this tool directly onto their Facebook or other social network profile page which will act as a deterrent to potential perpetrators.

Restricting access to unsuitable websites

The following websites are examples of those which pose threats to or may be unsuitable for young people and access may have to be restricted or denied by using appropriate filters

- Those which are sexually explicit or contain information of a sexual nature
- Those which permit the purchase of or promote the usage of drugs, alcohol or tobacco
- Personal and dating websites
- Age inappropriate chat rooms and social networking sites
- Certain gaming platforms and websites via X Box, Playstation, Wii etc
- Websites promoting eating disorders
- Websites promoting suicide
- Websites which teach criminal activities or skills including the purchasing, or enabling, of weapons and which advocate terrorism or extremism
- Those which portray or promote violence or inappropriate language including certain online gaming platforms
- Those which advocate hate speech about religion, race, nationality, gender, age disability or sexual orientation

Chat rooms and social networking sites

Depending on the age of the young person, access to chat rooms and social networking sites may not necessarily be restricted or prohibited (Facebook has a minimum age of 13), however those with parental consent should monitor which websites are being accessed and be familiar with the following risks before permitting access:

- People on the internet may not be who they say they are and may be trying to access young people via chatrooms in order to gain their trust and take advantage of them.
- Young people should also be encouraged to never give out any personal details or images which may identify themselves, their peers, their siblings / foster siblings, their location or any groups, schools or organisations they attend or associate with. This includes real names, dates of birth, address, phone numbers, e-mail addresses, photographs or videos, school attended, IM and email addresses, including those of friends, family / foster family and peers. This also includes any ‘gangs’ they may be affiliated with.
- Young people should not engage in risky behaviours on webcams as images can be shared with others, even by those they know – young people should be made aware that once an image is uploaded to the internet they no longer have control over it, irrespective of how quickly they try to remove the image.
- Young people should not meet up with strangers they have met online. Other internet users may not be who they claim to be and may have spent months ‘grooming’ a young person in order to gain their trust and take advantage of them. If however you

suspect that a young person does intend to meet up with someone you should advise them to always take someone else along with them and to meet in a busy public place such as a café or coffee shop and to stay there and under no circumstances, to go off with the person they have just met on their own..

Parents / carers and foster carers should only ever accept and confirm Facebook friend request from those already known to them.

Parents / carers and foster carers should ideally monitor their child's Facebook accounts and 'friends' lists (where possible).

Whilst for many families, Facebook, and other similar social networking sites, are a good way of keeping in touch and sharing information and photographs with other friends and family, this presents specific challenges and risks for foster carers in terms of safeguarding the young people they have temporary guardianship for.

In particular, foster carers should adhere to the following principles:

- Never upload photos of looked after children or their friends on to your Facebook profile.
- Never refer to the names of looked after children, their schools or the locations you go to with them or activities you do with them.
- Ensure your own children, other family members and friends follow the same principles and do not upload pictures of looked after children or refer to activities or locations they have been to with them.
- Never make reference to yourself as a foster carer on your Facebook profile.
- Ensure that your privacy settings are restricted to 'friends only'.
- Encourage your foster child(ren) to tell you about their positive and negative internet experiences. Work with them to help avoid future problems by finding solutions. Know what's 'cool' on the net and keep up with buzzwords, acronyms and latest trends.
- Always seek advice from the child's social worker in the first instance prior to permitting access to Facebook or any other social networking sites.

Gaming Platforms
In order to keep a young persons online gaming profile safe, age appropriate, fun and educational, parents / carers and foster carers should adhere to the following advice:

- Know the risks of online gaming:
    - Young people could download offensive content or viruses if they download games from unreputable websites
    - Some free games may require extensive profiles which game owners could then illegally sell on or exploit
    - Young people can be bullied and harassed online
    - Young people can be groomed online into meeting another player
    - Young people can become addicted to gaming, particularly Role Play games
- Explore online games together with the young person

  - Research and purchase online games with the young person only from reputable websites sticking to well known games which are age appropriate and suitable for all the family
  - Verify the game is age appropriate for the young person
  - Review and agree to the games terms and rules of play
  - Install family settings on games and explain to the young person why this is necessary

- Teach the young person basic rules for safer play
  - Verify how the sites privacy policy will protect information about young people
  - Agree on rules of play and set boundaries and time limits with the young person
  - Keep the gaming platform in a family room rather than the young person's bedroom. This also prevents young people playing games in the privacy of their bedroom after they have gone to bed
  - Only allow young people to play online when under supervision from a responsible adult
  - Advise young people never to share personal information about themselves, their families, their school or where they live. This includes the sharing of images of themselves.
  - Young people should not meet up with other online gamers unless they are already known to the young person
  - Password protect gaming accounts with complex passwords and create non suggestive family gaming names
  - Agree on fair play and to treat other gamers with respect and to trust instincts. If something doesn't feel right, then this must be raised with a responsible adult.

Please remember that there is a balance to be struck between freedom and protection, supervision and privacy and common sense. Children are looked after for a variety of reasons and very often, their foster families, schools and location have to be kept confidential from their birth families for their own safety and protection.

Foster Carers can refer to further Looked After Children guidance available from the young person's allocated social worker.

The following websites also provide additional useful advice for parents / carers and foster carers

Thinkuknow: www.thinkuknow.co.uk

Click Clever, Click Safe: clickcleverclicksafe.direct.gov.uk

Ofcom:http://consumers.ofcom.org.uk/2010/10/parental-controls-help-your-children-manage-their-media

Appendix 2

Cyber Bullying

It is essential that young people, professionals, parents / carers and foster carers understand how cyber bullying differs from other forms of bullying, how this can affect young people and what can be done to combat this form of abuse. Cyber bullying is just as harmful as bullying in the 'real' world and clear procedures should be in place to support the victim as well as respond to and manage the perpetrators actions.

It must be understood that as cyber bullying can happen 24 hours a day 7 days a week 365 days a year and at any time of the day or night, it differs from 'real world bullying as the victims cannot escape or find respite as it invades places that would ordinarily be safe and private spaces. Organisations must aim for the same 'zero tolerance' approach towards cyber bullying as they would for any other form of bullying.

Those who participate in online bullying often use groups of friends to target their victims. An action as innocent as adding derogatory comments to another person's photograph could rapidly spiral out of control and young people may not realise that their actions constitute bullying however the following are the most commonly reported :

- Email – Can be sent directly to an individual or group of people to encourage them to participate in the bullying and can include derogatory comments or harassment or examples of homophobia, racism, sexism or other forms of prejudice either by message or image. Something originally meant to be a joke can soon escalate out of control.

- Instant Messaging / Chat Rooms – Messages can be sent directly to an individual or group of people who can then be included in the conversation. Again, conversations can easily escalate out of control.

- Social networking sites – Anonymous profiles can be set up on social networking sites to make fun of someone and each person contributing to these pages can soon worsen the problem. Inappropriate and threatening comments and images can also be posted and circulated about individuals without their consent.

- Mobile phone – Anonymous and abusive text or video messages and photo messages and phone calls can be shared via mobile phones. This also includes the sharing of videos of physical and sexual attacks (which is a criminal offence) on individuals (includes happy slapping).

- Interactive gaming - Games consoles allow players to chat online with anyone they find themselves matched with in a multi-player game. Sometimes cyber bullies abuse other players and use threats. They can also lock victims out of games, spread false rumours about someone or hack into someone's account.

- Sending viruses – Viruses or hacking programs can be sent by one person to another in order to destroy their computers or delete personal information from their hard drive.

- Abusing personal information – Personal and sensitive information (including videos and photographs) could be uploaded onto the internet without the victims permission.

- Social networking sites such as Facebook make it very simple for other users to obtain personal information and photographs of others. They can also get hold of someone else's messaging accounts and chat to people pretending to be the victim.

Although cyber bullying of itself can not physically hurt a person, it can leave a young person mentally vulnerable, frightened and lonely and seemingly very difficult to escape from, particularly when this occurs in their own home and can lead to the bullied victim causing harm to themselves, which in some cases may escalate to suicide.

However some instances of cyberbullying are associated with or are linked to gang affiliation and 'real world' bullying and can rapidly escalate into physical retaliation as recent high profile violent (and sometimes fatal) cases highlight. These cases are stark reminders that cyberbullying cannot and must not be minimised.

There is no simple answer why some young people choose to bully other young people however all organisations working with young people should ensure they have recognised policies and procedures to challenge ***any*** form of bullying on their premises. Professionals should also be able to recognise signs and symptoms of bullying and have confidence in dealing with this.

All incidents of cyber bullying must be recorded and if necessary, escalated to the police if a criminal offence is suspected. (see Appendix 5). Young people should store the electronic records of abuse which will be essential in any subsequent investigation.

DoE and Childnet have produced resources and guidance that can be used to give practical advice and guidance on cyberbullying: http://www.digizen.org/cyberbullying

There is also an excellent award winning short film that helps sensitise people to the hurt and distress that can be caused by cyberbullying. The film shows ways in which cyberbullying can occur, who it involves, how it can affect different people, and what can be done to prevent it and respond to it.

http://www.digizen.org/resources/cyberbullying/films/uk/lfit-film.aspx

Appendix 3
LSCB E-Safety Sub-Group - Terms of Reference

- The development of an e-safety strategy to promote and safeguard the welfare of all Lambeth children when accessing the digital world.
- Ensuring that in the development of an e-safety strategy the membership of the sub committee is reviewed, extended and adjusted so that the work of the sub committee can be responsive to local need, changing or emerging technologies, national guidance and /or legislation.
- The development of model policies and procedures to promote and safeguard the welfare of children when using communication and digital technologies.
- Ensuring that all agencies recognise the importance of e-safety within the context of Every Child Matters
- Ensuring that e-Safety is embedded within safeguarding the policies, practices procedures and responsibilities of LSCB partners.
- Ensuring that all agencies providing services to children fulfill their duty to understand and deliver on e-Safety issues.
- Ensuring all agencies providing services to children promote children's safety online, whilst supporting adults who care for children.
- To ensure all agencies recognise that e-Safety is not just a technological issue.
- To develop training, education and information programmes as part of the e-Strategy, including communication and awareness raising.
- To develop an agreed procedure when responding to specific e-safety incidents.
- To monitor the impact of the e-Safety Strategy and supporting policies and procedures.
- To work in liaison with other LSCB committees and subgroups as appropriate.
- To liaise and work in partnership with other internal or external stakeholders or 'expert' agencies, such as CEOP as appropriate

Appendix 4
Safer working practices for adults working with technology with children & young people

Professionals (including volunteers) working with children and young people must appreciate that the nature and responsibilities of their professional roles place them in a position of trust with children and young people.

This appendix provides guidance to professionals who work with children and young people around safer working practices with technology and aims to:

- Ensure that children and young people are safeguarded in the digital world
- Provide professionals with advice and good practice to enable them to work safely and also to monitor their own practices by way of a culture of vigilance in the workplace
- Assist professionals to comply with their own Codes of Practice / Acceptable Use of Internet policies
- Minimise the risks of allegations of abuse or inappropriate behaviours being made against members of staff
- Project a clear message that unlawful or unsafe / risky behaviours with IDMT are unacceptable and that disciplinary action will be taken in line with other council policies

Employees may be investigated under the recognised disciplinary procedure for non-compliance but may initially be investigated by the Council under allegation protocols to consider whether they have harmed a child; committed a criminal offence towards a child; or have otherwise behaved in a manner towards a child(ren) that determines that they are unsuitable to work with or be in a position of trust with children. The outcome of such investigations is likely to be referred to the Independent Safeguarding Authority for consideration for barring from working with children

Frequently asked questions and answers

Q1 Should I use my personal mobile phone or camera to photograph or video children / young people I work with?

A No. Any photographic or video images of children / young people should always be recorded and stored on equipment belonging to the organisation after written consent from the parent/carer and with the agreement of the child/young person and the organisations senior management. Care must be taken to ensure that images are stored appropriately and securely.

If at any time you are witness to visible injuries or other signs of abuse or neglect (i.e.

bruising or scarring), you must not under any circumstances take any photographic images of this. Only medical staff and the Police Child Abuse Investigation Team (CAIT) are permitted to take photographic evidence.

Q2 Is it appropriate for me to continue to use my social networking sites?

A Professionals should review their personal content and ongoing usage of social networking sites as and when their professional responsibilities increase. Sound password and privacy settings should be applied (and regularly changed) in order for your profile and information about yourself to remain private. Friend requests from service users should be politely declined and as a rule of thumb, you should not publish any comments, images or comments about yourself or colleagues that you would not want your parents, children, family or employer to see either now or in ten years time.

Professionals should be aware that they should never under any circumstances post derogatory comments about their colleagues, their employer or service users as these could compromise their professional integrity and normally lead to disciplinary action by their employer.

Q3 Is it appropriate for me to have service users as friends on my instant messaging service?

A No. Professional boundaries have been overstepped and any communication with service users should always be made via appropriate channels in the working environment that can be scrutinised by management as necessary.

Q4 How can I ensure I am communicating with service users safely?

A Any communication between professional and service user should always (where possible) be made via equipment provided by the organisation in order for contact records to be logged and checked if necessary. Professionals should never use their personal email addresses, home addresses or personal telephone numbers to communicate with service users. This minimises the risk of allegations being made against the employee.

Q5 What is my responsibility for my work equipment (i.e. laptop / mobile phone) outside of my workplace?

A Unauthorised access to a wider network of websites by friends, family members and even strangers could increase the possibility of viral attacks, identity theft and inappropriate content being accessed / downloaded without your knowledge which you would be responsible and held accountable for. Personal and sensitive information about service users could also be accessed for inappropriate purposes.

Professionals accessing electronic work equipment outside of their normal workplace must therefore ensure they retain absolute control of this.

Q6 How can I store personal data safely?

A Electronic personal and confidential information must always be kept secure on hard drives or memory sticks but must be password protected and encrypted in line with the council's Acceptable Use of Internet & Data Protection policies.

Q7 As a technician, how can I safely monitor network usage?

A Filtering or recorded network usage can only be effective if monitored carefully to scrutinise and report inappropriate access, usage or storage of data as agreed by the council's ICT Departmental policies, with clear procedures to manage incidents to senior

management. Please refer directly to these for further information.

Appendix 5
Procedure for managing e-safety concerns