



**Knowsl@y Council**

**DCFS E-Safety Strategy / Acceptable Use Policy**

Version:	2.0
Policy Lead Officer	Leanne Hornsby
Consulted with:	HR, Graham Ennis Date: 21 <sup>st</sup> January 2010 IT, Andy Garden Date:27 <sup>th</sup> January 2010 Legal Services, Lyana Chan: 1 <sup>st</sup> February 2010 Learning Technologies Strategic Board: 24 <sup>th</sup> February 2010 E-Safety Working group: 11 <sup>th</sup> January 2010
Formally approved by:	Damian Allen, Executive Director of Children & Family Services  Signature: _____  Date: _____  Cllr Wright, Cabinet Member with portfolio responsibility for Children and Family Services  Signature: _____  Date: _____
In consultation with:	Mike Harden, Executive Director, Corporate Resources  Signature: _____  Date: _____  Cllr Keats, Cabinet Member with portfolio responsibility for Finance and Information and Technology  Signature: _____  Date: _____
Document Author:	Irene Tuzio
Name of responsible directorate:	Children & Family Services
Review date:	June 2010
Target audience:	Schools, Centres for Learning and other Education settings



## **Knowsley E-Safety Strategy 2010**

Knowsley Local Authority believes that the benefits of ICT and Internet use far outweigh the dangers. Recognising the issues and planning accordingly will help to ensure appropriate, effective and safe use for our children and young people, their parents/carers.

You can also get this information in other formats. Please phone Customer Services on 0151 443 3197, or email [customerservices@knowsley.gov.uk](mailto:customerservices@knowsley.gov.uk)

## Document Control:

### I Document History

Version	Date	Author	Change History
0.1	23/09/2008	I Tuzio	
1.0 Final	01/04/2009	I Tuzio	Feedback from ESWG
1.1	06/10/2009	I Tuzio	Feedback from ESWG
2.0	11/01/2010	I Tuzio	Feedback from ESWG and DCFS

### II References

Document Reference	Name (Location)
Kent County Council	Draft Schools e-Safety Policy 2007
The Northern Grid For Learning	Understanding E Safety and Managing the Risks
Leeds Safeguarding Children Board	E-safety Strategy for Leeds

### III Reviewers

No.	Reviewer Name	Date	Issue
1	ESWG		
2	KSCB		
3	DCFS		

### IV Document Approval

No.	Approver Name	Date	Issue
1	KSCB		
2			
3			

## **TABLE OF CONTENTS**

<b>FOREWORD</b>	<b>4</b>
<b>1 INTRODUCTION</b>	<b>5</b>
<b>2 SCOPE</b>	<b>5</b>
<b>3 KNOWSLEY SAFEGUARDING CHILDREN BOARD</b>	<b>5</b>
<b>4 WHY DEVELOP AN E-SAFETY STRATEGY?</b>	<b>6</b>
<b>5 WHAT IS E-SAFETY?</b>	<b>6</b>
<b>6 E-SAFETY STRATEGIC THEMES</b>	<b>7</b>
6.1 Policies, Practices and Procedures	7
6.2 Education and Training	8
6.3 Communication	8
6.4 Infrastructure and Technology	8
6.5 Standards and Inspection	9
<b>7 SUMMARY</b>	<b>9</b>
<b>APPENDIX 1 E-SAFETY PRIORITIES AND OBJECTIVES</b>	<b>11</b>

## **Foreword**

The world our children and young people live in is rapidly changing. New computer technologies are creating fantastic, exciting opportunities in communication, in learning and in many aspects of daily life. For a lot of adults these developments seem quite different from what we've seen before. This makes us naturally cautious about them. However, for young people they are a regular and familiar part of everyday life that are being enthusiastically embraced.

This gives those of us whose role it is to safeguard our children and young people new considerations and new responsibilities. We want them to flourish through the many benefits that Information Communication Technologies (ICT) offer. Yet at the same time we must help them understand and make informed decisions about what information they seek and share, the way they do this and who they do it with.

We are clear about this responsibility in Knowsley. Under the guidance of the E-safety Working Group of the Knowsley Safeguarding Children Board we have developed this, our E-safety Strategy, to give coherence and focus to our work. This strategy recognises our role in shaping the way young people access ICT, providing a safe environment. Crucially, it focuses on building the resilience of young people in using ICT, so they are equipped to enjoy the benefits and avoid the pitfalls and dangers.

The Children and Young People's Plan for Knowsley makes clear the approach we must take in developing our services. Our ICT Strategy is founded on Borough-wide connectivity to digital resources; facilities for digital resources to be easily created and amended; a Personalised Learning Environment (PLE) capable of delivering, creating and manipulating digital resources; and deployment of effective technical support to harness advantages.

We must personalise the support we provide so that each individual child or young person has the skills and understanding to use ICT safely. We must seek the participation of children, young people and families so we can appreciate the changing nature of their ICT usage and respond accordingly. We must work in partnership, to deliver a coherent approach with a particular focus on bringing our Centres for Learning, Schools and Children's Services together around this common agenda. Finally, we must come back to our responsibility – prevention – helping young people to ensure that they are able to identify, avoid and report dangers before they escalate.

This isn't always easy, the pace of change means that as adults we can be in danger of feeling out-of-touch with and confused by the technologies young people are using. However, the onus is on us to overcome these potential barriers and take a balanced, responsible view. ICT can bring huge advantages to children and young people's lives, We must help them to benefit from these safely and confidently.



**Damian Allen**

**Executive Director of Children and Family Services**

## 1 Introduction

Greater accessibility combined with the rapid pace of development means that ICT has penetrated into every aspect of young people's lives today. ICT is fast becoming the currency by which young people conduct their lives and their day to day activities. Few would dispute that the internet and other technologies have the potential to offer many positive benefits to young people. As with everything, this is not without risk. We want young people to be able to fully exploit the benefits offered by ICT while doing so in a safe manner.

## 2 Scope

Under section 11 of the Children Act 2004 and section 175 of the Education Act 2002), all professionals have a duty to safeguard and promote the well-being of all children. The duty of care to protect children and young people cannot be confined to a single environment but must extend to all environments in which they actively engage whether this is education settings, home, or the wider community. This requires an integrated approach across schools and other establishments that regularly come into contact with young people (herein after described as member agencies).

## 3 The Knowsley Safeguarding Children Board

The Knowsley Safeguarding Children Board (KSCB) takes seriously the statutory role it has to ensure that member agencies co-operate to safeguard and promote the welfare of children and young people in their locality, and to ensure that they are effective in doing so. As technology increasingly permeates into every aspect of a child's life from an ever younger age, e-safety must necessarily be part of this remit.

Through the implementation of this strategy KSCB and Stakeholders will work toward the aim of:

***'We as a Safeguarding Children Board will support Knowsley's children and young people and their families and carers to be safe in the e-world'***

The KSCB will be looking to stakeholders for their support and co-operation in developing an environment where children and young people can use the internet and other digital technologies safely.

In order to progress this work the KSCB has established a distinct E-Safety Working Group (ESWG) that reports directly to the KSCB/ Executive as recommended by BECTA to co-ordinate e-safety across the borough. The KSCB will ensure that best practice is developed, implemented and kept up to date.

## **4 Why develop an E-safety Strategy?**

Children's access to technology has increased phenomenally in recent years: ICT is embedded in reception classrooms and is a constant and prevalent feature of school life; home access is on the increase, while connectivity from public locations such as libraries and youth clubs is now commonplace. Equally, the convergence of technologies and decreasing cost of ownership mean that, with access to a whole range of online services from mobile phones to games consoles and similar devices, children are no longer restricted to accessing the internet from a fixed location.

While it is clear that technology offers children unprecedented opportunities to learn, communicate, create, discover and be entertained in a virtual environment, there are some inherent risks. And while most children's confidence and competence in using technologies is high, their knowledge and understanding of the risks may be low.

E-safety is widely discussed and commented upon, and there is a wealth of information available from a wide variety of sources for those who wish to learn more. Whilst this is positive, the abundance of such materials can mean that it is difficult to identify a single clear approach to pro-actively addressing e-safety. We recognise our role in providing the borough with a coherent and unified strategy for managing e-safety, whilst directing staff<sup>1</sup>, children and young people, their families and the public to a number of the excellent publications already available.

This e-safety strategy provides clarity both for young people, and all those who come into contact with them. It aligns with the outcomes of the Every Child Matters Agenda to safeguard and promote the welfare of children through the successful implementation of robust strategies and policies.

All agencies providing services to children have a duty to understand e-safety issues, recognising their role in helping children to remain safe online while also supporting adults who care for children.

## **5 What is E-safety?**

It must be recognised that e-safety is not a technological issue and is not limited to settings where children have access to technology. Likewise, responsibility for e-safety must not be delegated to technical colleagues or those with a responsibility for ICT, but must be firmly embedded within safeguarding policies, practices and responsibilities.

The Internet is an open communications channel, available to all. Applications such as the Web, e-mail, blogs and social networking all transmit information over the fibres of the Internet to many locations in the world at low cost. Anyone can send messages, discuss ideas and publish material with little restriction. These features of the Internet make it an invaluable resource used by millions of people every day.

---

<sup>1</sup> *staff includes all paid employees, including agency staff and volunteers*

Much of the material on the Internet is published for an adult audience and some is unsuitable for children and young people. In addition there is information that would be more restricted elsewhere, on subjects such as weapons, crime and racism. Children and Young People must also learn that publishing personal information could compromise their safety.

The law is catching up with Internet developments: it is an offence to store images showing child abuse and to use Internet communication to 'groom' children. Section 1 of the Computer Misuse Act 1990 makes it a criminal offence to "cause a computer to perform any function with intent to secure unauthorised access to any program or data held in any computer where that access is unauthorised and he knows at the time when he causes the computer to perform the function that that is the case". Knowsley must protect itself by making it clear to children, young people, staff and visitors that the use of council equipment for inappropriate reasons is "*unauthorised*".

This highlights the need to educate children and young people about the benefits, risks and responsibilities of using information technology, providing safeguards and awareness for users to enable them to control their online experiences.

Schools, colleges, children's centres, youth clubs, libraries, care homes and indeed all establishments which provide access to ICT must decide on the right balance between controlling access, setting rules and educating our children and young people on responsible use. Partner and Voluntary organisations must develop complementary strategies to ensure safe and responsible ICT use wherever young people may be. This requires an integrated approach across schools and other organisations that regularly come into contact with children and young people.

All staff who have contact with children and young people should promote the safe and responsible use of technology in its many forms. They should learn to recognise the behaviours in children that may indicate that they are at risk from e-safety issues, and know where to go for further help. Equally, all staff should be aware of the appropriate response if a child directly divulges an e-safety incident, how to assess the safeguarding implications and how to escalate it appropriately.

## **6 E-safety Strategic Themes**

### **6.1 Policies, Practices and Procedures**

A member of staff who flouts IT security advice, or uses email or the Web for inappropriate reasons risks dismissal. Clear guidance is needed for young people and all professionals who come into contact with them on what is deemed acceptable use. All staff should sign an Acceptable ICT Use Agreement on appointment. In signing, staff accept that their employer can monitor network and Internet use to help ensure staff and children and young people's safety. Acceptable use policies are fundamental to risk management.

An acceptable use policy must be wide ranging. It must consider both fixed and mobile access to the Internet, technologies provided by the service itself (such as PCs, laptops, mobile phones, webcams and digital video equipment) and

technologies owned by service users and staff but brought onto the service premises (such as mobile phones, camera phones, personal digital assistants (PDAs) and portable media players). It should be flexible enough to deal with new and emerging technologies, but should also recognise the important educational and social benefits of such tools.

Policies are of little value if practices and routines are not embedded within the culture of the organisation. Policies must be enforced and reviewed and systems must be monitored to ensure confidence in their effectiveness.

## **6.2 Education and Training**

No policy can protect our children and young people by itself. Staff vigilance in planning and supervising appropriate and educational ICT experiences remains essential.

Educating young people in the practice of acceptable use promotes responsible behaviour and builds resilience by providing an opportunity to reflect on some of the possible consequences associated with acting outside of these boundaries. The National Curriculum programme of study for ICT at Key Stages 1-4 also makes it mandatory for children and young people to be taught how to use ICT safely and securely. Together these measures form the basis of a combined learning strategy that can be supported by parents, carers, and staff who come into contact with children.

Resilience is key to e-safety, since we cannot realistically provide solutions to each and every potential issue arising in such a dynamic social and technical environment. Moreover we wish to preserve the right of individuals to fully explore the value and opportunity offered by ICT, which forms an inherent part of their development, whilst empowering them to keep themselves safe.

## **6.3 Communication**

Communication and Awareness Raising with parents and carers is essential as whilst educating our children and young people we must also educate and inform adults who are in regular contact with them. This includes the extended family.

Guidance therefore needs to be developed and communicated on awareness of e-safety issues with for example parents/carers and with staff working with children and young people, or on sites where children & young people may use or access ICT.

## **6.4 Infrastructure and Technology**

Infrastructure issues are just one aspect of an e-safety strategy but they are nonetheless vitally important. In technology-based services to children, a robust infrastructure can offer a first line of defence against e-safety risks, which must then be supplemented by the policy, education and standards aspects. Knowsley Safeguarding Children Board, through its E-safety Strategy, has a role to play in giving advice and guidance to member agencies on developing an e-safety

infrastructure. Although the Board has no operational control over the services which come under its remit, the focus should be on developing a set of core infrastructure principles which all children's services should aspire to achieve.

All KSCB member organisations are committed to delivering an ICT environment that is as safe and secure as possible. This includes standards for email and Internet filtering, anti-virus and anti-spam software, and ensuring that email addresses protect young people's anonymity.

We must continually rethink the technology shaping access to ICT and undertake risk assessments as new devices and methods of accessing information become available.

## **6.5 Standards and Inspection**

A framework for the regular audit of e-safety provisions within all settings across the borough must be in place. This should include qualitative analysis from children and young people as well as staff.

Monitoring and reporting on e-safety issues and incidents is important. Not only will it provide a permanent record of incidents, outcomes and actions taken, it will also provide an important tool for reflecting on and revising practice and for identifying emerging trends which can be addressed before they become problematic.

KSCB should seek to evaluate the effectiveness of its e-safety work through a peer-review process, based on self-evaluation, performance indicators and joint audit, while individual children's services and other member organisations continue to be assessed through their own quality and inspection regimes.

Proactive monitoring can be just as important to a successful e-safety strategy. Proactive monitoring of the digital landscape within a given area (for example, by determining the percentage of young people having Internet access at home or the percentage with social networking profiles) can help to establish how young people in the locality view and use digital technologies, what their concerns are, and any emerging issues. Not only will such proactive monitoring help to keep e-safety at the forefront of local thinking, but it can also produce key performance indicators with which to review and revise the E-safety Strategy in the future.

## **7 Summary**

Our aim is to develop safe and responsible users of ICT, and to educate those who come into contact with children and young people to identify and mitigate risk, and respond effectively to any incidents arising. The strategy requires schools and other learning organisations, parents, carers, pupils, and other professional organisations coming into contact with children and young people, to sign up to the principles contained within this document, and the policies underpinning it. Knowsley Safeguarding Children Board will support organisations in developing localised policies and practices aligned to this strategy, and scrutinise their effectiveness.

We will produce an E-safety Policy and guidance which will include a step by step guide on how incidents involving accessing of inappropriate material are dealt with, as well as an Internet Safety Self Review Framework, and a number of useful Internet safety links.

## Appendix 1

### E-SAFETY PRIORITIES AND OBJECTIVES

Strategic Priority	Objective
<p><b>Policies, practices and procedures</b></p>	<ul style="list-style-type: none"> <li>• To ensure that member agencies and partners of the KSCB, as well as other settings in which children and young people access the Internet and other digital technologies, have in place policies, procedures and practices that enable children and young people to use the Internet and mobile digital technologies safely.</li> <li>• To develop practice guidance related to Internet safety</li> <li>• Liaise with all partner agencies to develop generic and agency specific policies.</li> <li>• Ensure that policies and procedures to investigate and escalate e-safety incidents arising, adhere to wider safeguarding frameworks already in place, thus ensuring a co-ordinated and prompt response.</li> </ul>
<p><b>Education and training</b></p>	<ul style="list-style-type: none"> <li>• Develop an Education and Training Strategy that will ensure the provision of education to children and young people that promotes safe and responsible use of the Internet and other digital technologies. In addition, the strategy will include training for members of the children’s workforce with a view to raising their awareness of e-safety and how it relates to safeguarding children.</li> </ul>
<p><b>Infrastructure and technology</b></p>	<ul style="list-style-type: none"> <li>• Publish minimum standards relating to Internet provision, for use by all member agencies including schools.</li> <li>• Evaluate the benefits offered by logging and monitoring technologies in supporting secure access, and produce recommendations / directives as appropriate.</li> <li>• To develop and disseminate good practice information to stakeholders, aimed at enabling children and young people to use the Internet safely and responsibly</li> <li>• To develop a mechanism that will bring together experts in ICT and related technologies and also practitioners with a statutory duty to safeguard children to consider new and emerging technologies and their trends, and to disseminate good practice as quickly as possible to agencies providing services to children, young people and their families</li> </ul>
<p><b>Standards and inspection</b></p>	<ul style="list-style-type: none"> <li>• Ensure all schools and member agencies are equipped to identify e-safety risks and know when to escalate these.</li> <li>• Design and implement a monitoring framework</li> </ul>

	<p>to capture information about the volume and severity of ICT related e-safety incidents.</p> <ul style="list-style-type: none"> <li>• Develop a mechanism for sharing new national guidelines and local good practice relating to e-safety, and emerging trends captured through the monitoring framework.</li> <li>• Develop a framework for the regular audit of e-safety provisions within schools and other member agencies that includes qualitative analysis from staff and young people.</li> <li>• Evaluate the benefits offered by logging and monitoring technologies in supporting secure access, and produce recommendations / directives as appropriate.</li> <li>• To clarify the reporting mechanism for all member agencies and partners of the KSCB and to make it inclusive of the Internet Watch Foundation (IWF) and Child Exploitation Online Protection (CEOP) as well as the Police</li> </ul>
<p><b>Communications</b></p>	<ul style="list-style-type: none"> <li>• To develop a Media Strategy for dealing with child protection incidents</li> <li>• To audit the provision of e-safety training carried out and e-safety awareness campaigns by member agencies and partners with a view to ensuring consistency</li> <li>• To develop an awareness campaign that will focus on educating key stakeholders about the opportunities and the threats of the Internet and digital technologies</li> </ul>