## Contents

4 Foreword
6 Vision and Aims
8 Principles and Values
9 Scope
10 Needs Analysis
14 The Strategy
- Raising Awareness
- Building e-Safety Skills
- Creating e-Safer Communities
22 Monitoring and Evaluation
23 Appendices
- Appendix 1 Implementation Plan
- Appendix 2 Glossary of Terms
- Appendix 3. The Role of the e-Safety Lead
- Appendix 4. Key Contacts
- Appendix 5. Stakeholders Agreement
Foreword

Rapid developments in technology and online behaviour present excellent opportunities but also new risks to children and young people and vulnerable adults of online abuse, exploitation, exposure to explicit material, identity theft, grooming and cyber-bullying.

Dr. Tanya Byron’s 2008 report (‘Safer Children in a Digital World’), highlights the risks new technology presents to children and young people. Whilst innovations in technology are to be welcomed, embraced and celebrated stakeholders are under pressure to put in place e-Safety strategies which recognise the benefits of independent internet use whilst safeguarding from harm. It is therefore imperative that measured precautions are put in place and priority given to this area of safeguarding as robustly as in others.

This Strategy is Suffolk’s response to safeguarding and promoting the welfare of our ‘Digital Natives’, those children and young people who are life long users of modern technology. It also seeks to provide an overarching umbrella for the development and provision of advice, information and awareness, to help to safeguard vulnerable adults, parents, carers and those that work with those groups.

This will enable innovations in modern technological advances continuing to be enjoyed by our children and young people, as we strive to minimise the risks posed to
them in these virtual communities as robustly as we would in our real communities.

In line with national policy developments and evidenced based research in this area, our partner’s including children, young people and their families have welcomed the steps we are taking to build e-Safer communities.

This is a live document, which will develop in response to changes in national policy and expectations, and be refined as a result of ongoing consultation, monitoring and evaluation.

It also recognises that the audiences who may use this strategy are diverse. Rarely will one approach fit all, and that there are many things which will best be achieved in relation to e-Safety when carried out in partnership. By adopting this strategy we seek to support organisations using it to engage their staff and service participants to ensure it remains current and fit for purpose.

Graham Newman
Chair of Children Trust Partnership
This strategy is an attempt to both celebrate modern technological advances whilst also recognising the need to build our children, young people and vulnerable adults’ skills and resilience in Suffolk. We also need to ensure that they are properly protected from what could be used as a new avenue of potential harm.

Vision and Aims

Share the vision to:

- Safeguard and promote the welfare of vulnerable groups in this digital age.
- Understand e-Safety issues and recognise their role in protecting children and young people whilst online and supporting adults who care for children.
- Recognise that e-Safety encompasses a range of technology including the internet and hand held devices.
The strategy seeks to address the following aims and objectives:

**Aim**
To ensure that every child and young person and vulnerable adults in Suffolk is aware and builds resilience in e-Safety, in order to stay safe.

**Objectives**

1. Raise awareness of the importance of e-Safety in promoting the safeguarding and welfare of children and young people and vulnerable adults.
2. Increase everyone’s understanding that e-Safety is wider than just a technological issue.
3. Develop information, guidance, support and training in e-safety for key stakeholders including children, young people, vulnerable adults and their families.
4. Monitor, review and improve the e-Safety Strategy to ensure its impact and ongoing effectiveness.

The strategy will build on good practice. It focuses particularly on actions to deliver key expectations, such as:

- Raising awareness.
- Developing skills.
- Building children, young people and vulnerable adult’s resilience.
- Monitoring activity.
- Responding appropriately to abuse.
- Developing e-Safer communities.
The strategy recognises that children and young people are digital natives and have extensive experience in the use of modern technology. They have a lot to offer in the way of knowledge, information and insight into the potential benefits and dangers associated with its use.

The knowledge of children and young people can add value to the design and delivery of services and we acknowledge the involvement of children and young people and vulnerable adults in the development of this strategy.

To achieve our aims everyone needs to sign up to the shared values, behaviours, principles and outcomes to keep children and young people and vulnerable adults safe whilst using developing technology. Therefore everyone will need to operate within a set of values which provide:

- The safeguarding and welfare of children, young people and vulnerable adults.
- Respect and accept diversity.
- Trustworthiness.
- Honesty and integrity.
- Listening and understanding.
- Consistency and fairness.
Scope

This strategy seeks to include and involve:

- Children and Young People.
- Parents and Carers.
- Staff and Volunteers who work with Children and Young People.
- Vulnerable Families.
- Other Vulnerable Adults.
- Seldom Heard Groups.
- Strategic Leaders.
- Service Providers.
- Commissioners/ Policy Makers.
- Commercial World.
- Statutory Organisations.
- Voluntary Organisations.
- The Media.
- Training Providers.
- Schools and Education Settings.
Suffolk has around 160,000 children and young people under 19 years of age, which represent 25% of the population. The projection of older people is set to rise by 189,000 by 2020 (by over 50%) and vulnerable adults accounting for at least (78%) of this projection with 140,000 adults with physical disabilities and approx 3,000 with severe learning disabilities. For vulnerable adults the main e-Safety issues appear to be the risk of financial abuse, fraud and identity theft including online fraud. 

Breaches of e-Safety are most likely to occur among young people of primary school age and upwards. The most common breach is the viewing of unsuitable online material.

Current research has found that where children and young people were taught about e-Safety, all breaches of e-Safety were reduced. Breaches are also more likely to occur when young people are allowed to bring their own personal equipment (such as laptops, portable storage devices and internet enabled mobile phones) onto school premises.

In some cases, such as incidents of bullying via mobile phones, breaches are not only more likely to occur, but also occur with greater frequency when mobile phones are allowed on to school premises.

Ofcom in a national study, (2008 - 2009) estimated that 99% of those in the seven to seventeen age group accessed the internet.
Dr. Tanya Byron in her report ‘Safer Children in a Digital World’ 2008 recognised that children and young people are at ease and confident with their use of new technologies.

Whilst it was found that both children and their parents enjoyed the use of the internet, children were worried about the following:

- That they might come across something rude or scary.
- They might experience unwelcome contact from other internet users including cyber bullying.
- How others including younger siblings behaved online.

Their parents were concerned that:

- They did not always understand how to use technology or how to manage the technology as well as, or better than their children.
- Parents and teachers regard inappropriate contact on the internet as one of the online risks for children.
- The time their children and young people were spending online including online gaming.

A key finding was that children and young people do not always have the knowledge, skills and understanding to keep themselves safe in the online world.
The Childwise research also undertaken in 2008 found that 90% of children aged 5-16 have internet access at home. This is set to increase with national initiatives such as the Home Access programme.

In Suffolk 180 young people contributed to the Staying Safe consultation in July 2010. The consultation found that 40% of our young people had met new people in chat rooms and had met these new people face-to-face. In comparison to the national return, the outcome suggested that children and young people in Suffolk were more at risk than those surveyed in the more recent Child Exploitation and Online Protection (CEOP) centre research undertaken in 2007.

From 6000 young people in the CEOP survey aged 11-16 years, 25% had met a new ‘friend’ from the internet in real life.

Around 1 in 13 children aged 11-16 have been persistently cyber bullied in the last year, while 40% of young people aged 13-18 know friends who engage in ‘sexting.’ (Ofcom 2008/2009)
The development of the strategy has taken account of the needs analysis and the following detail of the strategy seeks to address Suffolk’s vision for keeping our children, young people and vulnerable adults safe whilst using modern technology as well as raising awareness of the issues and to develop the skills and confidence of both children and adults in responding to these concerns.

1 Suffolk County Council Adult and Community Services Joint Strategic Needs Assessment 2007

2 Ofcom’s response to the Byron Review, Ofcom, 2008; www.ofcom.org.uk/research/telecoms/reports/byron/

3 Safer children in a digital world: the report of the Byron Review, [PP/D16 (7576)/03/08], DCSF and DCMS, 2008; www.dcsf.gov.uk/byronreview/
The Strategy

The strategy is divided into three key aims for e-Safety across Suffolk. These are:

- **Raising Awareness**

  **AIM:** That everyone including children and young people, their families, vulnerable adults and those who work with them are aware of the potential safeguarding issues and know where to go for advice, information and support.

- **Building e-Safety Skills**

  **AIM:** To ensure all children and young people and vulnerable adults in Suffolk remain safe and act responsibly whilst using developing technology including the internet and online gaming facilities.
Creating e-Safer Communities

AIM: To create e-Safer communities where e-Safety is embedded in everyone’s policies, commissioning and planning activities, in order to prevent and appropriately respond to safeguarding matters.
Raising Awareness

‘Raising awareness, sharing information, giving support’.

AIM: That everyone including children and young people, their families, vulnerable adults and those who work with them are aware of potential safeguarding issues and where to go for advice, information and support.

Those engaging in the strategy will seek to:

- Raise the awareness of everyone to the e-Safety agenda and Suffolk’s response through a range of activities that provide services, advice, information, guidance, support and training.
- Engage everyone by creating joint learning opportunities in the safe use of developing technology.
- To raise awareness by equipping parents, carers and families in being able to support and protect children and young people and vulnerable adults.
Good Practice Highlights:

**Safe-T-Net** http://safetnet.org.uk

Safe-T-Net provides advice and training to staff and parents connected with youth organisations, such as:

- Schools (both primary and secondary).
- Youth groups.
- Sports clubs.
- Church groups.

**UCS** also runs TUK (Think U Know) training. Interested delegates need to first register with CEOP at www.thinkuknow.co.uk. As well as teaching delegates how to deliver TUK products to young people, this free training will also increase their understanding of many of the most popular applications young people are using in the online and mobile environment. The course covers many issues that children and young people face online and signposts to initiatives and organisations for help and support.
Building e-Safety Skills

‘Building resilience, creating capacity, staying safe’

AIM: To ensure all children, young people and vulnerable adults in Suffolk remain safe and act responsibly whilst using developing technology including the internet and online gaming facilities.

- Develop the awareness and risk assessment skills of children, young people and vulnerable adults to minimise risks and ensure they know what to do when faced with issues (Including cyber bullying, child abuse and online fraud).

- Build on and use the skills and experiences of our digital natives to encourage their positive contribution in keeping themselves and their peers safe and to promote the responsible use of technology.

- Develop and make available tools for parents/carers and those working or offering services to children, young people and vulnerable adults, which will equip them with the necessary skills, knowledge and support to help keep them safe when using ICT.
Good Practice Highlights:

On the 30th June 2009, colleagues met with young people from secondary schools, 1 middle school and 2 special schools to look at issues around; cyber bullying, bullying in school and bullying in the community.

This conference was filmed by ‘I made this’ which included interesting results that questioned our perceptions of bullying and emphasised the need for a cluster based anti-bullying policy. This film was shown to the Northern Area Managers network where positive feedback was received.

In the autumn term, a longer film project is planned; to be designed and implemented by young people that can be shown in schools in North Lowestoft. The intention is to follow this up with a shared policy for schools and shared marketing campaign with the hope of targeting bullying from primary school onwards and instilling a ‘no tolerance’ culture in schools.

University Campus Suffolk have developed a flexible 12 week course which examines current key debates on children, young people and new media technologies. Children’s perspectives are central to this course and considered within a variety of topical themes. This course also provides up to date e-safety training from CEOP and EPICT and provides participants with the opportunity to gain 20 credits at Master’s level.
Creating e-Safer Communities

‘Creating e-Safer communities, embedding good practice, safeguarding from harm’

**AIM:** To create e-safer communities where e-Safety is embedded in everyone’s policies, commissioning and planning activities in order to prevent and appropriately respond to safeguarding matters.

The organisations involved in the strategy must:

- Develop policies and procedures in order to safeguard and promote the welfare of all children, young people and vulnerable adults in Suffolk.
- Develop robust systems for preventing e-Safety breaches, for reporting and recording concerns with clear thresholds for statutory responsibility.
- Monitor the development and evaluate the impact of our strategy for keeping children, young people and vulnerable adults safe.
- Nominate e-Safety Leads with the expertise and knowledge to respond to requests for support from children, young people, families, vulnerable adults and organisations when dealing with e-Safety issues.

**Good Practice Highlights:**

Suffolk Local Safeguarding Children Board produced an e-Safety information leaflet for parents, carers to know what to do if concerned about a child and an e-Safety issue.
We will assist in updating and assessing the impact of our strategy, by:

- Assessing the impact of the policy and processes to ensure it meets with Equality Standards, Diversity and other relevant requirements.
- Devising a framework which enables all stakeholders to provide feedback on the quality of services and the strategy, using a range of communication methods.

- Require an annual audit of e-Safety practices to be undertaken by the e-safety officer, linked to the scrutiny and quality assurance function of the Local Children and Adult Safeguarding Boards in order to inform policy development, improvements in practice and training.
- Looking at Lessons learnt from Serious Case Reviews where concerns are linked to e-Safety issues and use outcomes to inform policy, planning, practice, learning and development.
Appendices

Appendix 1: Implementation Plan
Appendix 2: Glossary of Terms
Appendix 3: The Role of the e-Safety Lead
Appendix 4: Key Contacts
Appendix 5: Stakeholder Agreement
Objective 1: Raise the awareness of young people, their parents, carers, and vulnerable adults to the e-safety agenda and Suffolk’s response through a campaign of activities that provides services, advice, information and guidance in relation to e-Safety.

Appendix 1: Implementation Plan

Raising Awareness

**AIM:** That everyone including children, young people, their families, vulnerable adults and those who work with them are aware of potential safeguarding issues when using developing technology and where to go for advice, information and support.

<table>
<thead>
<tr>
<th>Actions/Milestones</th>
<th>Lead</th>
<th>By When</th>
<th>Outcomes</th>
</tr>
</thead>
<tbody>
<tr>
<td>To have developed an e-Safety strategy, policy framework and model policy where appropriate, for use in all organisations including the voluntary sector.</td>
<td>LSCB e-Safety sub group.</td>
<td>November 2010</td>
<td>For all organisations to have e-Safety included as an integral part of their safeguarding policy and procedures.</td>
</tr>
<tr>
<td>To deliver or contribute to an e-Safety conference in Suffolk to launch the strategy and implementation plan.</td>
<td>LSCB e-Safety sub-group and partners</td>
<td>Feb 2011 Safer Internet Day</td>
<td>To engage a wide audience in the launch of Suffolk’s e-Safety strategy</td>
</tr>
</tbody>
</table>
Objective 1 continued

<table>
<thead>
<tr>
<th>Actions/Milestones</th>
<th>Lead</th>
<th>By When</th>
<th>Outcomes</th>
</tr>
</thead>
<tbody>
<tr>
<td>To develop a communication strategy using customer segmentation to deliver</td>
<td>LSCB e-Safety sub-group</td>
<td>Jan 2011</td>
<td>To communicate the e-Safety strategy to a wide variety audience to raise awareness.</td>
</tr>
<tr>
<td>appropriate messages in collaboration with the Communications service.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>To promote the annual national ‘Safer Internet Day’ locally.</td>
<td>Partner Organisations/e-Safety leads.</td>
<td>ongoing</td>
<td>To raise awareness of the ‘Safer internet day’ as an integral part of the wider safeguarding agenda and promote all organisations housing the CEOP report button in the commitment to safeguarding children, young people and vulnerable adults.</td>
</tr>
</tbody>
</table>
Objective 2: Engage children, young people, parents, carers and vulnerable adults in joint learning opportunities in the safe use of modern technology.

<table>
<thead>
<tr>
<th>Actions/Milestones</th>
<th>Lead</th>
<th>By When</th>
<th>Outcomes</th>
</tr>
</thead>
<tbody>
<tr>
<td>To map existing resources and training availability.</td>
<td>Suffolk Children’s Trust/LSCB Training Sub-group QA process.</td>
<td>Year 1 and 2 (Teachers from 60 schools to be trained by Summer term 2011). 25 e-safety ambassador/cyber mentors.</td>
<td>For all schools and organisations to have a trained e-Safety ambassador/Cyber-mentor able to deliver the e-safety/cyber mentor programme to children, young people, their parents and carers.</td>
</tr>
<tr>
<td>To develop a training strategy to meet identified needs.</td>
<td></td>
<td></td>
<td>For every child, young person, parent, carer and vulnerable adult to have the opportunity to engage in e-safety training/awareness sessions across Suffolk.</td>
</tr>
<tr>
<td>To monitor and evaluate e-Safety training in each of the local areas in ‘Building e-Safety skills’.</td>
<td></td>
<td></td>
<td>To develop integrated working around parental engagement.</td>
</tr>
<tr>
<td>Actions/Milestones</td>
<td>Lead</td>
<td>By When</td>
<td>Outcomes</td>
</tr>
<tr>
<td>----------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------</td>
<td>------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Disseminate information leaflets for parents and carers.</td>
<td>LSCB/ Adult Safeguarding Board/ Suffolk’s Children’s Trust.</td>
<td>Ongoing</td>
<td>To disseminate local e-Safety information leaflet for parents and carers to inform and advise on e-Safety issues.</td>
</tr>
<tr>
<td>Advise all organisations where mobile/wireless technology is available of the need for an e-Safety lead and e-Safety policies as part of their safeguarding arrangements through the development of role description to be widely circulated.</td>
<td>e-Safety Officer/CYP Safeguarding in Education service/ Adult Safeguarding Board/LSCB e-Safety sub-group reps.</td>
<td>Year 1 ongoing</td>
<td>To ensure all organisations have robust safeguarding arrangements and that Management Committees/Governing bodies and providers are aware of their responsibilities. Ensure schools and other organisations include e-Safety as part of the safeguarding training as well as by formal notification, communications strategy and appropriate representation on the e-Safety sub-group.</td>
</tr>
</tbody>
</table>
## Objective 2 continued

<table>
<thead>
<tr>
<th>Actions/Milestones</th>
<th>Lead</th>
<th>By When</th>
<th>Outcomes</th>
</tr>
</thead>
<tbody>
<tr>
<td>To QA and monitor delivery of awareness sessions in the community/voluntary sector aimed at families, children, young people, vulnerable adults and their carers.</td>
<td>Suffolk Children’s Trust/ LSCB PMQA, Adult Safeguarding Board in collaboration with CEOP ambassadors.</td>
<td>Ongoing</td>
<td>To increase knowledge, skills and understanding in e-Safety issues.</td>
</tr>
<tr>
<td>Public awareness raising activities.</td>
<td></td>
<td></td>
<td>To support children and young people, their parents, carers and those that work with them building e-Safety skills.</td>
</tr>
</tbody>
</table>
## Building e-safety Skills

**AIM:** To ensure all children and young people in Suffolk remain safe and act responsibly whilst using technology including the internet and online gaming facilities.

### Objective 1:

To develop the awareness, and risk assessment skills of children and young people and vulnerable adults in order to ensure they know what to do when faced with cyber bullying and other forms of abuse from the use of modern technology.

<table>
<thead>
<tr>
<th>Actions/Milestones</th>
<th>Lead</th>
<th>By When</th>
<th>Outcomes</th>
</tr>
</thead>
<tbody>
<tr>
<td>To engage a representative group of young people and vulnerable adults by developing a shadow strategy group of young people and vulnerable adults for young people and vulnerable adults on e-safety.</td>
<td>LSCB e-Safety sub-group/ Suffolk Children Trust.</td>
<td>Year 1-3</td>
<td>To work with a mixed group of young people year 3 and above to design and print an e-Safety poster, Suffolk DVD and easy guide to the strategy for launch at the safer internet day.</td>
</tr>
</tbody>
</table>
## Objective 1 continued

<table>
<thead>
<tr>
<th>Actions/Milestones</th>
<th>Lead</th>
<th>By When</th>
<th>Outcomes</th>
</tr>
</thead>
<tbody>
<tr>
<td>To map training capacity by collating a list of trained CEOP Ambassador Trainers across Suffolk.</td>
<td>E-Safety Officer and Local e-Safety Leads LSCB e-Safety sub group</td>
<td>Year 1-3</td>
<td>For all settings to have e-Safety Ambassadors/cyber mentor to be able to offer peer mentoring, support and training to other young people who might be experiencing or at risk of cyber bullying and child abuse.</td>
</tr>
<tr>
<td>To develop Young e-Safety Peer Ambassadors to raise awareness through peer support, advice and consultation.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

## Objective 2: Develop resources for parents/ carers and those working or offering services to children and young people and vulnerable adults, which will equip them with the necessary knowledge and support to help keep children, young people and vulnerable adults safe when using ICT.
<table>
<thead>
<tr>
<th>Actions/Milestones</th>
<th>Lead</th>
<th>By When</th>
<th>Outcomes</th>
</tr>
</thead>
<tbody>
<tr>
<td>To create a website presence for e-Safety resources linked to Suffolk LSCB site and other Partner organisations web sites.</td>
<td>e-Safety sub Group/Suffolk e-safety Officer.</td>
<td>Year 1-2</td>
<td>To ensure all people working with children, young people and vulnerable adults know where to find e-Safety resources.</td>
</tr>
<tr>
<td>To create opportunities for designated e-Safety leads and advisors to have access to appropriate training in order to gain skills and confidence in dealing with e-safety issues effectively.</td>
<td>LSCB e-Safety sub group/ Suffolk Children Trust. QA through LSCB training sub-group.</td>
<td></td>
<td>That the CEOP report abuse button is widely available on websites in the county.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Ensure schools and organisations using tools for Parental Online Reporting to gain specific support.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>To develop expertise across the county to respond effectively to e-Safety issues when raised.</td>
</tr>
</tbody>
</table>
Objective 1: Develop robust systems for reporting concerns with clear thresholds for response and intervention.

Creating e-Safer Communities.

**AIM:** To create e-Safer communities where e-safety is embedded in everyone’s policies, commissioning and planning activities in order to prevent and appropriately respond to safeguarding matters.

<table>
<thead>
<tr>
<th>Actions/Milestones</th>
<th>Lead</th>
<th>By When</th>
<th>Outcomes</th>
</tr>
</thead>
<tbody>
<tr>
<td>To develop an e-Safety incident reporting procedures which outlines the actions that will be taken in the event of breaches of e-Safety.</td>
<td>LSCB e-safety sub-group.</td>
<td>Year 1-3</td>
<td>To equip all organisations with a tool that appropriately identifies and responds effectively to an e-Safety incident.</td>
</tr>
<tr>
<td>To develop appropriate response interventions where they relate to children and Young People under the age of 18 years.</td>
<td></td>
<td></td>
<td>To adopt a countywide protocol that reduces the criminalisation of young people through delivery of appropriate alternative responses by schools and other agencies through education.</td>
</tr>
</tbody>
</table>
Objective 2: Develop robust systems for reporting concerns with clear thresholds for response and intervention.

<table>
<thead>
<tr>
<th>Actions/Milestones</th>
<th>Lead</th>
<th>By When</th>
<th>Outcomes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Raise awareness of the CEOP button through multi-agency training.</td>
<td>LSCB/Suffolk Children’s Trust/ Adult Safeguarding/</td>
<td>Year 1-3</td>
<td>To ensure all children, young people and vulnerable adults have appropriate access to report concerns and that agencies can keep them safe whilst accessing the internet.</td>
</tr>
<tr>
<td>Request all e-Safety champions lead on this.</td>
<td>Suffolk e-safety Officer/ All local e-Safety leads.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Monitoring and Evaluation

“Learning lessons, assessing impact and monitoring performance”

**AIM:** To ensure a full integration and implementation of e-Safety as an integral part of all organisations policies, procedures and practice.

**Objective 1:** To monitor the use of modern technology and the impact of keeping children, young people and vulnerable adults safe.
## Appendix 1: Implementation Plan

<table>
<thead>
<tr>
<th>Actions/Milestones</th>
<th>Lead</th>
<th>By When</th>
<th>Outcomes</th>
</tr>
</thead>
<tbody>
<tr>
<td>To develop an incident recording and reporting procedures.</td>
<td></td>
<td></td>
<td>To provide a clear process for recording monitoring and responding to e-Safety breaches across the county.</td>
</tr>
<tr>
<td>To implement an annual e-Safety audit process for monitoring e-Safety arrangements in all organisations.</td>
<td></td>
<td></td>
<td>To produce annual reports arising from outcomes of integrated e-Safety self-review audits in order to inform policy, planning, commissioning, service delivery and support.</td>
</tr>
<tr>
<td>To implement knowledge share sessions and lessons learnt literature arising from e-Safety incidents and serious case reviews and audits where findings include issues of e-Safety.</td>
<td></td>
<td>March 2011</td>
<td>For all organisations involved with children, young people and vulnerable adults to learn from evidence based practice and improve safeguarding arrangements as an outcome.</td>
</tr>
<tr>
<td>To present report findings to the LSCB PM&amp;QA, Adult Safeguarding Board and Children Trust arising from learning events, e-Safety incidents and serious case review and audits.</td>
<td>Local e-Safety leads.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

**e-Safety Officer**

---

---

---
Appendix 2: Glossary of Terms

In this document, as in the Children Act 1989 and the Children Act 2004, a child is defined as anyone who has not yet reached their eighteenth birthday. Where we use the word ‘child’ (or its derivatives) in this document, we mean ‘child or young person’.

We have taken the definition of a vulnerable adult to mean anyone aged 18 years or older who is living in residential or sheltered accommodation, receiving domiciliary or health care, is detained or receiving welfare services or requires assistance in the conduct of his or her own affairs. A vulnerable adult may also be receiving direct payments and receiving or participating in services specifically targeted at people with age-related needs, disability or mental health conditions.

Terms such as, ‘online’, ‘Information Communication Technologies’, ‘digital technologies’, and ‘modern technology’, are used interchangeably to describe modern technology including: mobile phones, laptop computers and online gaming equipment and other wireless enabled or hand held devices.
CEOP
www.ceop.gov.uk
The Child Exploitation and Online Protection (CEOP) Centre the UK’s national law enforcement agency focusing on internet safety.

Commercial World
Private enterprise business communities and social enterprises.

Cyber space
Describes the online computer generated/virtual world.

Cyber-bullying
This is the harassment, maltreatment or discrimination of another through the use of mobile technology including text messaging, or social network sites or mobile phones.

Digital Natives/ Silent Generation
Is a term used to describe children and young people who have had a long life use of modern technology. As Dr Byron had described in her 2008 report: ‘For them, new technologies are a seamless part of the world into which they were born.’

E2BN
www.e2bn.org
E2BN is the Learning Grid for the East of England and regional provider of the National Education Network.

Sexual Exploitation
Abuse of power by a coercive adult and can include material or financial gain.
- **Exposure to explicit material**
  This is where a child or young person could discover or experience sexually revealing or illegal material usually of a pornographic nature.

- **Grooming**
  This is a term used to describe the preparing or priming of a child or young person in order to abuse them.

- **Identity theft**
  Where someone’s personal details such as name, address, bank details are stolen to commit a criminal offence e.g. fraud.

- **LSCB**
  Local safeguarding Children Board is a key statutory mechanism for agreeing how relevant organisations co-operate to safeguard and promote the welfare of children.

- **PMQA**
  Performance Monitoring and Quality Assurance is a sub-group of the LSCB and monitors the quality of safeguarding arrangements of relevant organisations.

- **Seldom Heard Groups.**
  This is a term used to describe groups of people that often get left out when organisations involve their users or customers, such as:
- People who do not frequently engage in public consultations.
- Minority groups, such as non-English speaking people, people from black and minority ethnic communities, gay men and lesbians and homeless people.
- Young people, older people and people living in rural communities.
- Hidden communities such as drug users, sexually active teenagers and sex workers.
- Vulnerable groups that may require different ways of communicating, such as people with learning difficulties, those with a visual impairment and people with a mental illness.

- Faith groups.
- People who are just uninterested and/or disillusioned.

**Sexting.**
Is the slang term used for the use of a mobile phone or other similar electronic device to distribute pictures or video of sexually explicit images. It can also refer to text messages of a sexually charged nature.

**Thinkuknow**
www.thinkuknow.co.uk
Thinkuknow is an education initiative by the Child Exploitation and Online Protection (CEOP) Centre.
A named e-Safety lead role is crucial to the process of developing and maintaining an e-Safety culture within an organisation and has specific responsibility for overseeing each of the elements of the PIES model:

- Policies and practice,
- Infrastructure and technology,
- Education and training and
- Standards and Inspection.

We must stress that e-Safety is not about ICT. Therefore it will not be appropriate to delegate all responsibility to a member of the technical staff. The named e-Safety lead must have the authority to call upon other staff within the organisation to assist them in their role.

Key Responsibilities of an e-Safety Lead:

- Developing an e-Safety culture under the direction of the management team and acting as a named point of contact on all e-Safety issues.
- Ensuring that everyone including children and young people know what to do if they are concerned about an e-Safety issue.
- Ensuring that e-Safety is embedded within continuing professional development (CPD) for staff and coordinating training as appropriate.
- Ensuring that e-Safety is embedded across all activities as appropriate.
Ensuring that e-Safety is promoted to parents and carers, other users and children and young people of ICT resources and supporting them in their understanding of the issues.

Maintaining an e-Safety incident log (Additional Guidance forthcoming).

Monitoring and reporting on e-Safety issues to the management team, and other agencies as appropriate.

Developing an understanding of the relevant local and national guidance.

Liaising with the local authority, Police, IWF, (Internet Watch Foundation www.iwf.org.uk) and CEOP (Child Exploitation and Online Protection Centre www.ceop.police.uk) as appropriate.

Reviewing and updating e-Safety policies and procedures on a regular basis and after an incident.

Ensure that local outcomes and feedback are shared internally and externally via the Local e-Safety Lead Officer

Ensuring that the infrastructure and Technology provides a safe and secure environment for children and young people.

NB. False Alarms are Acceptable!
Appendix 4: Key Contacts

For more information on the e-safety strategy contact:

Lorna Jackson
Professional Advisor/e-Safety Officer
at lorna.jackson@suffolk.gov.uk

The e-safety sub group has representation from the following organisations:
(in alphabetical order)

- Broke Hall Primary School
- CSD
- E2BN
- Great Cornard High School
- Safe child
- Suffolk County Council
- Suffolk New College
- Suffolk Police
- Suffolk Youth and Connexions
- University Campus Suffolk
- Young Suffolk
Useful websites:

- www.e2bn.org
- www.thinkuknow.co.uk
- www.bnetsavvy.org
  Is a comprehensive internet safety website providing up to date information about online trends and behaviour and offers practical cyber safety tools for use in the home and classroom.

- www.education.gov.uk
  Becta is the government agency leading the national drive to ensure the effective and innovative use of technology throughout learning. The website archive can be found on the Department for Education at the above address.

- www.kidsmart.org.uk
  website resource for children, young people on being internet smart

- www.nextgenerationlearning.org.uk
  Government campaign initiated by Becta to make learning more exciting, rewarding and successful through the use of technology.

- www.childnet-int.org
  A non-profit organisation working with others to “help make the internet a great and safe place for children”.
Appendix 5: Stakeholders Agreement

All organisations who have signed up to the strategy will evidence their commitment and support to the strategy by adding their logo below.
The Voice of Children and Young People

Over 140 children and young people joined in at the Safer Internet Day (SID) 2011 held at the University Campus Suffolk. The following comments were captured from over 45 children and young people in response to two questions poised about the strategy: These are their responses...

What was good about the strategy?

- It helps people understand that the internet is not entirely safe and that you cannot trust everyone that adds you.
- It protects you from bad people online who want your details and stops you from revealing your details.
- It helps people/children to stay safe when on the internet.
- Because it is teaching us to stay safe on the internet.
- Because it keeps children safe on the internet.
- It helps people understand that the internet is not entirely safe and that you cannot trust everyone that adds you.
What would make it even better?

- If everyone in the world could see it and then use it.
- Make it so younger children can understand to.
- A warning came up if someone tried to contact you.
- See what sites we are on and maybe block them if they are inappropriate.
- If your parents could control it.
- If all schools got taught e-Safety.
- Well for starters it was fantastic but you could get some young children that have seen this and talk to other new people.
- If you keep to the rules and use it more.
For more information on the e-safety strategy contact: **Lorna Jackson**
Professional Advisor/e-Safety Officer
at lorna.jackson@suffolk.ov.uk