

# Emerging Digital and Mobile Technologies and Child Abuse

## Introduction

**12.1** This chapter focuses on the emergence of digital and mobile technologies and their impact upon children and young people in terms of child protection and safeguarding. The chapter aims to provide agencies with information regarding the emergence of Web 2.0 technology (that is use of the internet by individuals to create and distribute their own content) and how it can be used facilitate the abuse children and young people.

**12.2** The chapter only acknowledges digital and mobile technology that is currently in wide use. However, it is recognised that there are emerging digital technologies that will undoubtedly provide greater access to children and young people, which could possibly lead to their exploitation.

**12.3** Background information regarding the types of risk to children and young people through digital and mobile technologies is provided in the *Practice Guidance section of the website*.

## Responding to examples of e-incidents

**12.4** It is recognised that, the nature and level of ICT technology and the way in which it can cause harm to children and young people cannot be underestimated. Moreover, the way in which agencies respond to e-incidents can vary according to the level of risk posed to a child or young person, and also the organisational and technical infrastructure that is in place to monitor and respond to incidents.

**12.5** There are a series of procedures that exist which will underpin the response of agencies to e-incidents, these are:

- The individual dealing with the e-incident should follow existing safeguarding procedures which include Chapters 5 (Child Protection Enquiries and Related Criminal Investigations); 9 (Abuse by Children and Young People) and 13 (Allegations against a person who works with, or is in contact with children in a work or care setting, including volunteers), which will include the normal procedural processes of a strategy meeting, a child protection conference (if it is assessed as necessary to protect a child or young person and promote his/her welfare).
- Any hardware needs to be isolated and taken away to ensure that it is not modified. This means unplugging the computer and any accompany hardware and then placing them in a secure environment.

- Where communication has taken place in the form of chat logs/emails, these should be saved to a secure place e.g. on a CD ROM **or** in a secure drive on the agency IT network, the secure drive should be set up to ensure that there is limited access to it.
- Where an organisation is aware that its network has been used to either access or forward indecent images and there is a failure to act, this could be interpreted as possession, leaving individuals open to prosecution.
- It should be recognised that behaviour which starts off as inappropriate may develop into illegal activity due to the persistent, deliberate and upsetting nature of the communication received. In such circumstances the agency should seek advice from the Police.
- Ensure that all e-incidents are logged using the e-incident log sheet. These sheets should be stored in a confidential fashion and reviewed on a regular basis, as part of monitoring patterns and behaviours of use. If a pattern does emerge, details should be shared with either the Police, CSC or the LADO and advice sought.
- Information which will help determine whether a specific e-incident is illegal or inappropriate can be found in the 'Glossary of Current Legislation'.

Below is a table that looks at the range of key e-incidents and the subsequent responses according to the type of user

***Children and Young People***

Type of incident	Example	Review how it happened	Response
<b>Accidental access to inappropriate material</b>	Searching for an image for school work: <ul style="list-style-type: none"> <li>• In the classroom</li> <li>• In the public library</li> </ul>	<ul style="list-style-type: none"> <li>• Was it accidental?</li> <li>• Inappropriate search term used?</li> <li>• Word misspelt?</li> <li>• Using an online resource which gives wide access to images e.g. Google Image?</li> <li>• Has copyright been breached?</li> </ul>	<ul style="list-style-type: none"> <li>• Review filtering level</li> <li>• Use of open resources that are copyright free</li> <li>• Consider more appropriate search terms/keywords</li> <li>• Written record to be completed by the supervising adult who then reports to their manager</li> <li>• Designated Senior Person for Child Protection informed</li> <li>• Inform parent that inappropriate material accessed</li> <li>• Detail of URL taken for blocking purposes</li> <li>• Fill out comprehensively and clearly the e-incident log sheet</li> </ul>
<b>Deliberate access to inappropriate material</b>	Using a known inappropriate term when undertaking a Google search (web or images)	<ul style="list-style-type: none"> <li>• What happened?</li> <li>• When did it happen?</li> <li>• How was it accessed?</li> <li>• Was the individual going round the firewall using a proxy server?</li> <li>• Use of specific terminology?</li> </ul>	<ul style="list-style-type: none"> <li>• Written record to be completed by the supervising adult who then reports to their manager</li> <li>• Inform parent that inappropriate material accessed</li> <li>• Review filtering level and other safeguards</li> <li>• Details of URL taken for blocking</li> </ul>

			<p>purposes</p> <ul style="list-style-type: none"> <li>• Fill out clearly and comprehensively the e-incident log sheet</li> </ul>
<b>Accidental access to illegal material</b>	Indecent images of children	<ul style="list-style-type: none"> <li>• Record how it was accessed (where it is, process gone through to get there)</li> <li>• How did you become aware of it?</li> <li>• Who is responsible for accessing it?</li> </ul>	<ul style="list-style-type: none"> <li>• <b>Isolate equipment</b></li> <li>• Fill out clearly and comprehensively the e-incident log sheet</li> <li>• <b>Report it to the police immediately and inform Children Social Care (CSC)</b></li> </ul>
<b>Deliberate access to illegal material</b>	Indecent images of children received from a third party	<ul style="list-style-type: none"> <li>• Where did you see it?</li> <li>• Who is responsible?</li> <li>• How do you know it is deliberate access?</li> </ul>	<ul style="list-style-type: none"> <li>• <b>Isolate equipment</b></li> <li>• Do not let the alleged perpetrator know you are aware</li> <li>• Record details of how you came across it</li> <li>• Fill out clearly and comprehensively the e-incident log sheet</li> <li>• <b>Report it to the police immediately and inform CSC</b></li> </ul>
<b>Inappropriate or illegal use of email</b>	Fraud or running a business that sees children exploited sexually or otherwise	<ul style="list-style-type: none"> <li>• Does the incident constitute inappropriate or illegal use?</li> <li>• Does the email constitute unsolicited communication?</li> <li>• Who is responsible for sending the email?</li> <li>• How was the incident brought to your attention?</li> </ul>	<ul style="list-style-type: none"> <li>• Record details of the sender and recipient</li> <li>• Record the total number of emails sent and received</li> <li>• <b>Secure the communication in a safe place e.g. CD or IT network</b></li> <li>• Fill out clearly and comprehensively the e-incident log sheet</li> </ul>

		<ul style="list-style-type: none"> <li>• By who and when?</li> </ul>	<ul style="list-style-type: none"> <li>• Where the incident is deemed inappropriate it should be dealt with according to the organisation's existing policies related to behaviour management, acceptable use policy (AUP) etc</li> <li>• Where the incident is deemed illegal <b>report it to the police immediately and inform CSC</b></li> </ul>
<b>Deliberate misuse of the network</b>	Hacking Virus propagation Using the organisation's network to host a website	<ul style="list-style-type: none"> <li>• What happened?</li> <li>• How was the network accessed?</li> <li>• What damage has been done to the network?</li> <li>• Have people outside the organisation been affected?</li> <li>• How much of the network has been affected?</li> <li>• Has the integrity of the network been compromised?</li> </ul>	<ul style="list-style-type: none"> <li>• Fill out clearly and comprehensively the e-incident log sheet</li> <li>• Assessment to be undertaken by the organisation's IT Department</li> <li>• <b>Report it to the police immediately and inform CSC</b></li> </ul>
<b>Bullying or harassment using technologies</b>	Instant Messaging Email Social networking sites Video exchange sites Mobile phones Hand held games with wireless connection Personal digital assistants	<ul style="list-style-type: none"> <li>• Is the communication unsolicited?</li> <li>• What technology(ies) is(are) being used?</li> <li>• Who made the initial report – victim or bystander?</li> <li>• What is the nature of the bullying?</li> </ul>	<ul style="list-style-type: none"> <li>• Record details of the sender and recipient</li> <li>• Can you be certain of the identity of the sender and the recipient?</li> <li>• Record the total number of emails sent and received</li> <li>• <b>Secure the communication in a safe place e.g. CD or IT network</b></li> </ul>

			<ul style="list-style-type: none"> <li>• Fill out clearly and comprehensively the e-incident log sheet</li> <li>• Where the incident is deemed inappropriate it should be dealt with according to the organisation's existing policies related to behaviour management, acceptable use policy (AUP); Anti-bullying policy; racist incidents reporting procedure etc</li> <li>• Where the incident is deemed illegal <b>report it to the police immediately and inform CSC</b></li> </ul>
<b>Sexual exploitation using technologies</b>	Grooming through social networking sites, online gaming, email, instant messenger, video exchange and webcams	<ul style="list-style-type: none"> <li>• How has the incident been identified?</li> <li>• Who informed you?</li> <li>• What services were used e.g. social networking site?</li> <li>• On how many occasions has contact been made?</li> <li>• What is the time period for the exchange of communication?</li> </ul>	<ul style="list-style-type: none"> <li>• Fill out clearly and comprehensively the e-incident log sheet</li> <li>• <b>Report it to the police immediately and inform CSC</b></li> </ul>

Below is a table that looks at the range of key e-incidents and the subsequent responses according to the type of user

***Adults working with children and young people***

Type of incident	Example	Review how it happened	Response
<b>Access to inappropriate material</b>	Searching for an image for work: <ul style="list-style-type: none"> <li>• In the classroom</li> <li>• In the public library</li> </ul>	<ul style="list-style-type: none"> <li>• Inappropriate search term used?</li> <li>• Word misspelt?</li> <li>• Using an online resource which gives wide access to images e.g. Google Image?</li> <li>• Has copyright been breached?</li> </ul>	<ul style="list-style-type: none"> <li>• Written record to be completed by the supervising adult who then reports to their manager</li> <li>• Detail of URL taken for blocking purposes</li> <li>• Fill out comprehensively and clearly the e-incident log sheet</li> <li>• Designated Person for Child Protection provided with e-incident sheet and advice sought from CSC, Police</li> <li>• Inform the Allegations Management LADO (Local Authority Designated Officer) of the incident and subsequent action taken</li> </ul>
<b>Access to illegal material</b>	Indecent images of children Indecent images of children received from a third party	<ul style="list-style-type: none"> <li>• Where was it seen?</li> <li>• Who was using the computer/digital technology at the time?</li> </ul>	<ul style="list-style-type: none"> <li>• <b>Isolate equipment</b></li> <li>• Do not let the alleged perpetrator know you are aware</li> <li>• Fill out clearly and comprehensively the e-incident log sheet</li> <li>• Designated Person for Child Protection informed</li> <li>• <b>Report it to the police immediately</b></li> </ul>

			<p><b>and inform CSC</b></p> <ul style="list-style-type: none"> <li>• Inform the Allegations Management LADO (Local Authority Designated Officer) of the incident and the subsequent action taken</li> </ul>
<b>Misuse of email</b>	Fraud or running a business that sees children exploited sexually or otherwise	<ul style="list-style-type: none"> <li>• Does the incident constitute inappropriate or illegal use?</li> <li>• Does the email constitute unsolicited communication?</li> <li>• Who is responsible for sending the email?</li> <li>• How was the incident brought to your attention?</li> <li>• Is the sender using his/her own details or has he/she set up fake information to mask his/her identity?</li> <li>• If so what evidence do you have for this?</li> </ul>	<ul style="list-style-type: none"> <li>• Record details of the sender and recipient</li> <li>• Record the total number of emails sent and received</li> <li>• Secure the communication in a safe place e.g. CD or IT network</li> <li>• Fill out clearly and comprehensively the e-incident log sheet</li> <li>• Where the e-incident involves <i>another adult</i> contact HR department and discuss an appropriate response.</li> <li>• Inform the Allegations Management LADO of the incident and subsequent action</li> <li>• Where the e-incident involves a <i>child/young person</i> contact the Allegations Management LADO (Local Authority Designated Officer)</li> </ul>
<b>Misuse of the network</b>	Hacking Virus propagation Using the organisation's	<ul style="list-style-type: none"> <li>• What happened?</li> <li>• Do you know how the network accessed?</li> </ul>	<ul style="list-style-type: none"> <li>• Fill out clearly and comprehensively the e-incident log sheet</li> <li>• Assessment to be undertaken by the</li> </ul>

	network to host a website	<ul style="list-style-type: none"> <li>• Can you specify what damage has been done to the network?</li> <li>• Have people outside the organisation been affected?</li> <li>• How much of the network has been affected?</li> <li>• Has the integrity of the network been compromised?</li> </ul>	<p>organisation's IT Department</p> <ul style="list-style-type: none"> <li>• <b>Report it to the police immediately and inform CSC</b></li> <li>• Inform the Allegations Management LADO of the incident and subsequent action</li> </ul>
<b>Bullying or harassment using technologies</b>	<p>Instant Messaging Email Social networking sites Video exchange sites Mobile phones Hand held games with wireless connection Personal digital assistants</p>	<ul style="list-style-type: none"> <li>• Is the communication unsolicited?</li> <li>• What technology(ies) is(are) being used?</li> <li>• Who made the initial report – victim or bystander?</li> <li>• What is the nature of the bullying?</li> </ul>	<ul style="list-style-type: none"> <li>• Record details of the sender and recipient</li> <li>• Record the total number of emails sent and received</li> <li>• Secure the communication in a safe place e.g. CD or IT network</li> <li>• Fill out clearly and comprehensively the e-incident log sheet</li> <li>• Where the e-incident involves <i>another adult</i> contact HR department and discuss an appropriate response.</li> <li>• Inform the Allegations Management LADO of the incident and subsequent action</li> <li>• Where the e-incident involves a <i>child/young person</i> contact the Allegations Management LADO (Local Authority Designated Officer)</li> </ul>

<b>Sexual exploitation using technologies</b>	Grooming through social networking sites, online gaming, email, instant messenger, video exchange and webcams	<ul style="list-style-type: none"> <li>• How has the incident been identified?</li> <li>• What services were used e.g. social networking site?</li> <li>• On how many occasions has contact been made?</li> <li>• What is the time period for the exchange of communication?</li> </ul>	<ul style="list-style-type: none"> <li>• Fill out clearly and comprehensively the e-incident log sheet</li> <li>• <b>Report it to the police immediately and inform CSC</b></li> <li>• Inform the Allegations Management LADO of the incident and subsequent action</li> </ul>
---	---	---	--

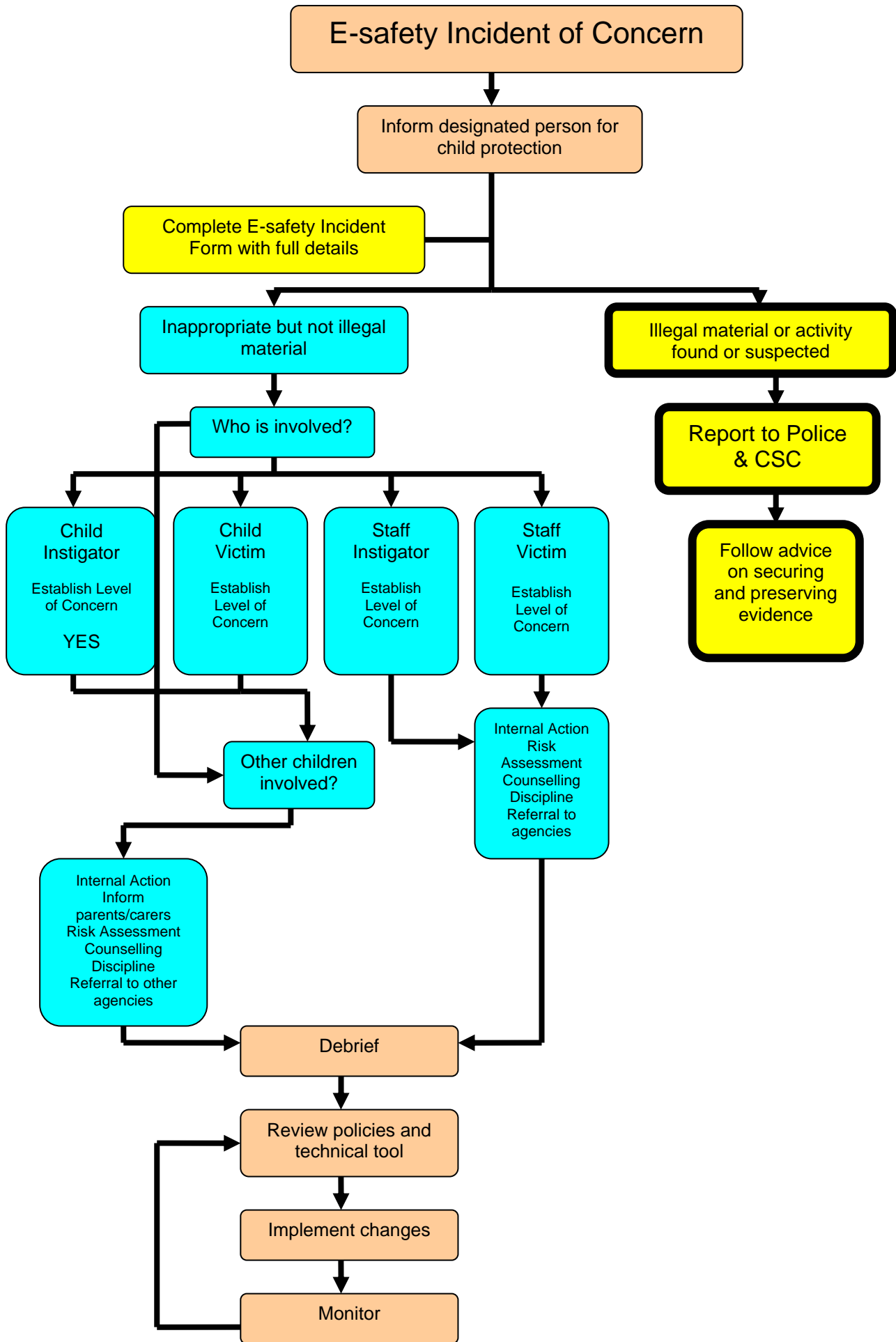
Below is a table that looks at the range of key e-incidents and the subsequent responses according to the type of user

***Children and Young People who may have been subject to harm***

Type of incident	Example	Review how it happened	Response
<b>Access to inappropriate material</b>	Searching for an image for school work: <ul style="list-style-type: none"> <li>• In the classroom</li> <li>• In the public library</li> </ul>	<ul style="list-style-type: none"> <li>• Was it accidental?</li> <li>• Inappropriate search term used?</li> <li>• Word misspelt?</li> <li>• Using an online resource which gives wide access to images e.g. Google Image?</li> <li>• Has copyright been breached?</li> </ul>	<ul style="list-style-type: none"> <li>• Review filtering level</li> <li>• Written record to be completed by the supervising adult who then reports to their manager</li> <li>• Designated Senior Person for Child Protection informed</li> <li>• Inform parent that inappropriate material accessed</li> <li>• Detail of URL taken for blocking purposes</li> <li>• Fill out comprehensively and clearly the e-incident log sheet</li> <li>• <b>Report it to the police immediately and inform Children Social Care (CSC)</b></li> </ul>
<b>Access to illegal material</b>	Indecent images of children	<ul style="list-style-type: none"> <li>• Record how it was accessed (where it is, process gone through to get there)</li> <li>• How did you become aware of it?</li> </ul>	<ul style="list-style-type: none"> <li>• <b>Isolate equipment</b></li> <li>• Fill out clearly and comprehensively the e-incident log sheet</li> <li>• <b>Report it to the police immediately and inform Children Social Care (CSC)</b></li> </ul>

<b>Inappropriate or illegal use of email</b>	Fraud or running a business that sees children exploited sexually or otherwise	<ul style="list-style-type: none"> <li>• Does the incident constitute inappropriate or illegal use?</li> <li>• Does the email constitute unsolicited communication?</li> <li>• Who is responsible for sending the email?</li> <li>• How was the incident brought to your attention?</li> <li>• Is the sender using his/her own details or has he/she set up fake information to mask his/her identity?</li> <li>•</li> </ul>	<ul style="list-style-type: none"> <li>• Record details of the sender and recipient</li> <li>• Record the total number of emails sent and received</li> <li>• <b>Secure the communication in a safe place e.g. CD or IT network</b></li> <li>• Fill out clearly and comprehensively the e-incident log sheet</li> <li>• <b>Report it to the police immediately and inform CSC</b></li> </ul>
<b>Misuse of the network</b>	Hacking Virus propagation Using the organisation's network to host a website	<ul style="list-style-type: none"> <li>• What happened?</li> <li>• Do you know how the network accessed?</li> <li>• Can you determine what damage has been done to the network?</li> <li>• Have people outside the organisation been affected?</li> <li>• How much of the network has been affected?</li> <li>• Has the integrity of the network been compromised?</li> </ul>	<ul style="list-style-type: none"> <li>• Fill out clearly and comprehensively the e-incident log sheet</li> <li>• Assessment to be undertaken by the organisation's IT Department</li> <li>• <b>Report it to the police immediately and inform CSC</b></li> </ul>
<b>Bullying or harassment using technologies</b>	Instant Messaging Email Social networking sites Video exchange sites	<ul style="list-style-type: none"> <li>• Is the communication unsolicited?</li> <li>• What technology(ies) is(are) being used?</li> <li>• Who made the initial report –</li> </ul>	<ul style="list-style-type: none"> <li>• Record details of the sender and recipient</li> <li>• Record the total number of emails sent and received</li> </ul>

	<p>Mobile phones Hand held games with wireless connection Personal digital assistants</p>	<p>victim or bystander?</p> <ul style="list-style-type: none"> <li>• What is the nature of the bullying?</li> </ul>	<ul style="list-style-type: none"> <li>• Secure the communication in a safe place e.g. CD or IT network</li> <li>• Fill out clearly and comprehensively the e-incident log sheet</li> <li>• <b>Report it to the police immediately and inform CSC</b></li> </ul>
<p><b>Sexual exploitation using technologies</b></p>	<p>Grooming through social networking sites, online gaming, email, instant messenger, video exchange and webcams</p>	<ul style="list-style-type: none"> <li>• How has the incident been identified?</li> <li>• What services were used e.g. social networking site?</li> <li>• On how many occasions has contact been made?</li> <li>• What is the time period for the exchange of communication?</li> </ul>	<ul style="list-style-type: none"> <li>• Fill out clearly and comprehensively the e-incident log sheet</li> <li>• <b>Report it to the police immediately and inform CSC</b></li> </ul>



## E-incident Log Sheet – Part One

<b>To be completed as thoroughly as possible by the member of staff identifying the incident.</b>			
<b>Date(s) of incident:</b>			
<b>Time(s) of incident:</b>			
<b>Duration of incident:</b> <i>(e.g. First one, a week, 6 months etc.)</i>			
<b>Description of the e-safety incident:</b> <i>include detail of specific services or websites used (e.g. chat room, instant messenger); email addresses; usernames etc.</i>			
<b>Why do you have concerns about this incident?</b>			
<b>Has the information been recorded and secured?</b>	<b>Yes</b>		<b>No</b>
<b>Has any computer or hardware been secured?</b>			
<b>If yes, how and where, who by and when?</b>			
<b>Who was involved and how do you know this? Is there any evidence to suggest that false names/details have been given?</b> <i>Give full details of real names and email addresses etc where known.</i>			
<b>How was the incident identified?</b> <i>E.g. by member of staff, informed by third party, identified by IT dept. etc.</i>			
<b>What actions were taken, and by whom?</b> <i>Give detail of agencies informed and contact person within those agencies.</i>			
<b>Name of person completing this form:</b>			
<b>Organisation:</b>			
<b>Date:</b>		<b>Signature:</b>	
<b>Send this form immediately to the person with responsibility for child protection within your organisation.</b>			

### E-incident Log Sheet – Part Two

To be completed by the person with responsibility for child protection within the organisation.

Conclusions to the incident:

Have specific vulnerabilities or trends been identified?

Yes

No

If yes, what action will now be taken?

Name of receiving officer:

Date: