



Bromley E-safety Strategy 2009 - 2011

Date: January 2009

Strategy Review Date December 2011

Contents

INTRODUCTION	3
The Issue	3
Position Statement.....	3
Audience.....	4
Local Structure – E-safety in Bromley	4
STRATEGY.....	5
Purpose of the Strategy	5
Strategic objectives	5
Strategic Priorities.....	7
Priority Objectives.....	7
MONITORING AND EVALUATION	9
USEFUL CONTACTS	9
BROMLEY E-SAFETY ACTION PLAN	10
Annex 1: Glossary of Terms and Acronyms used in the document.....	11
Annex 2: Key drivers.....	12
Annex 3: Interdependencies	13
Annex 4 Example Network Account Agreement – Student.....	14
Annex 5 Example Network Account Agreement (Staff).....	15
Annex 6: E-Safety Audit Template	16
Annex 7: Membership & Governance.....	17

INTRODUCTION

The Issue

Today's children are citizens of a digital world. The use of the internet and digital technologies are integral to their physical world. Their emotional lives and their development are bound up in the use of these technologies. Children's relationship to information, their methods of entertainment and, perhaps most importantly, their means of communication are digitally enabled.

Most parents and carers will be experiencing these changes as a revolution. For some it may be a disempowering one and a barrier to communication with their children rather than an aid. The safeguarding challenge is to consider the well being of children and young people in terms of their relationship to technology and risks that exist. Bromley Safeguarding Children Board has a statutory duty to safeguard and promote the welfare of children in their locality.

This document sets out the Bromley Safeguarding Children Board's response to this challenge and our strategic direction for 2008 - 2011.

Position Statement

"Swimming pools can be dangerous for children. To protect them, one can install locks, put up fences and deploy pool alarms. All of these measures are helpful, but by far the most important thing that one can do for one's children is teach them to swim."

*'Youth, Pornography and the Internet'
National Research Council USA 2002*

When thinking of safety, technological solutions are not enough. Teaching a child to swim not only may prevent them from drowning, it gives them pleasure and benefits their health. Teaching children about the safe use of the internet, helps to ensure their safety and contributes to their emotional health and enjoyment of the world. Esafety is about balancing opportunities with risks.

This strategy aims to minimize the risks. It aims to achieve this through encouraging children and young people to develop as responsible online citizens.

STRATEGY

Purpose of the Strategy

The purpose of developing this strategy document and developing an e-safety work-stream is to:

- To build on the work of Becta, the Home Office and CEOP in raising awareness about the safe use of information communication technologies by children.
- To take a lead role in the development and delivery of training and education programmes (including linking with CEOP)
- To devise an overarching e-safety strategy that forms the basis for other local agency strategies.
- To support all agencies involved in the safeguarding of children in developing policies, procedures and strategies related to e-safety.
- To ensure that the LSCB monitors that strategies are in place through the Policy Procedures and Communication Sub-Committee.

Strategic objectives

The objectives of the BSCB are:

- Be a central point of contact for guidance, advice and networking on developing e-safety policies, strategies and communication to partner agencies.
- Identify e-safety contacts who work within their agencies to raise awareness and understanding. Facilitate this through appropriate web – based information.
- Develop audit reporting guidance and forms making effective use of existing systems and processes.
- Provide training or information about available training that to support the development of E-safety key contacts in agencies:
 - Professionals with direct contact with children and young people and those managing services for children young people and their carers.
 - Youth Council representatives
 - LSCB Board members
 - School Designated CP Leads
- Identify and signpost available resources and where necessary develop them e.g.

- Awareness raising resources for children and young people
 - educational resources for teachers
 - resources aimed at educating parents
 - Signpost appropriate web filtering/monitoring tools
- Provide expertise in developing a strategy, policy, and action plan in agencies
 - Provide information about current developments in the field through news updates and the BSCB website.
 - Lobby relevant groups to raise the profile of e-safety within the borough (e.g. with Children's Strategic Partnership Board).
 - Promote the safety of data, in terms of collection, storage and use as identified in the London Child Protection Procedures including use of Contact Point, the storage and security of information about children and young people.
 - Monitor e-safety arrangements of partners and provide audit tools

BSCB agencies' and other stakeholders' e-safety contacts will:

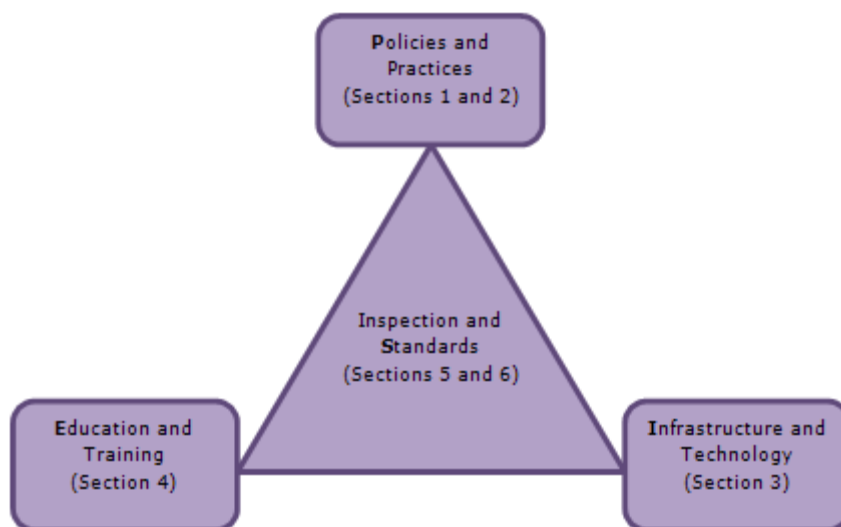
- Attend training on e-safety
- Be a point of contact for any e-safety safeguarding issues including the development of strategies in their agencies
- Be part of a reporting structure for responding to incidents
- Encourage staff in their agency to attend multi-agency BSCB e-safety training
- Raise awareness through the dissemination of information within their agency
- Build e-safety information into communications developed for the public (where appropriate e.g. Health Visitors' information packs for young mothers, use of contact point and sharing of information)

LSCB board members

- Nominate e-safety contacts within their agencies
- Support the development of strategies and policies within their agencies

Strategic Priorities

The BSCB identified six strategic priorities informed by the PIES model that agencies will engage in taking forward.



PIES model for limiting e-safety risks

The six priorities are:

1. Raise awareness and understanding of esafety issues amongst children and young people
2. Raise awareness and understanding of esafety issues amongst parents and carers
3. Raise awareness and understanding of esafety issues across all member agencies
4. Enable all member agencies to respond appropriately to incidents as well as to respond to risks posed to children and young people
5. Improve safety of children and young people's access to the internet
6. Monitor e-safety arrangements and incidents in the borough

Priority Objectives

This section sets out the objectives related to each priority area.

1. Raise awareness and understanding of esafety issues amongst children and young people
 1. Enable all schools to tackle the issue of esafety
 2. Improve the effectiveness of esafety awareness raising in schools – increased pupils aware
 3. Increase availability of esafety educational resources to pupils outside mainstream education
 4. Make esafety a talking point for children and young people outside of the school environment
 5. Increase the number of professionals who are aware of esafety issues

2. Raise awareness and understanding of e-safety issues amongst parents and carers
 1. Improve levels of awareness amongst parents and carers of the risks posed to children and young people by their use of technology
 2. Improve levels of awareness amongst parents and carers of ways of mitigating the risks posed to children and young people
 3. Improve awareness amongst parents and carers of available resources in this area
 4. Increase awareness of how to respond and report incidents both to local and national agencies

3. Raise awareness and understanding of e-safety issues amongst all member agencies
 1. Increase the number of teachers and non teaching staff in schools with an understanding of the issues and how to deal with them
 2. Increase the number of professionals with an understanding of the importance of esafety and how to deal with the issues
 3. Use e-safety contacts within agencies to disseminate information about esafety to staff.
 4. To continue to raise the profile of esafety amongst professionals
 5. Obtain broad commitment to esafety at executive level beyond the BSCB

4. Enable all member agencies to respond to the risks posed to children and young people by their use of ICT.
 1. Where appropriate, agencies have esafety strategies in place. These should cover their responsibilities for educating children, responding to and investigating incidents, protecting staff, storing information securely.
 2. All agencies have such esafety policies appropriate to their individual circumstances
 3. Enable rapid multi-agency responses to esafety incidents
 4. Ensure that esafety incidents are recognized and escalated as appropriate

5. Improve safe access to the internet for children and young people
 1. Obtain an overview of young people's points of access to the internet
 2. Improve the safety of children's use of the internet in the home
 3. Improve the safety of children's use of the internet in schools
 4. Improve the safety of children's use of the internet in non school environments
 5. Improve the safety of children's use of the internet in commercial internet access points (e.g. internet cafes)

6. Monitor e-safety arrangements in Bromley
 1. Gather an accurate and up to date picture of e-safety arrangements in all member agencies
 2. Gather an accurate and up to date picture of e-safety arrangements in schools
 3. Gather qualitative information on young people's opinions about esafety arrangements and current risks
 4. Monitor the number of ICT related child protection incidents quarterly
 5. Monitor the nature and range of ICT related child protection incidents annually

Role of Agencies

Agencies to develop:

- E-safety
- anti-bullying policies
- recording systems
- monitoring plans
- awareness raising plans

MONITORING AND EVALUATION

The strategy and accompanying action plan will be monitored annually by Bromley Safeguarding Children Board. Each agency will be expected to record incidents of harm through digital technology. The BSCB expects agencies to report annually on the number of incidents and on the arrangements in place to ensure that children and young people are adequately safeguarded. The outcomes from the monitoring and the evaluation process will be used to inform planning and targeting of resources.

USEFUL CONTACTS

For further information on this Strategy contact:

List your organisation's key contact for E-safety here:

Include

- name
- job title
- address
- phone
- email address

BSCB E-Safety Contact

Yvonne Onyeka
Development Officer, BSCB
Rm 40 St Blaise Building
Civic Centre
Bromley
BR1 3UH
0208 461 7563

www.bromleysafeguarding.org

[bscb website](#)

BROMLEY E-SAFETY ACTION PLAN

Activity	Timeline	Responsible
1 Raise awareness and understanding of e-safety issues amongst children and young people.		
Engage Children and Young people in developing awareness raising materials. <ul style="list-style-type: none"> • E-safety Day • E-safety competition in schools and youth services Development of publicity material for school children. <ul style="list-style-type: none"> • bookmarks 	10 Feb 09 Feb- Mar Feb – May 2009	E-safety Task Group DP & HB BSCB
2 Raise awareness and understanding of e-safety issues amongst parents and carers.		
Communicate E-safety message through Board information: <ul style="list-style-type: none"> • Safe Parenting Handbook Signpost parents to information about E-safety. <ul style="list-style-type: none"> • BSCB website Young People produce information to share with parents and carers on e-safety <ul style="list-style-type: none"> • Competition Assess the feasibility of an on line teaching module – use by parenting skills providers & children’s centres	Jan 09 Reception Yr3. On going Mar 09	YO/NB YO AF/SS
3 Raise awareness and understanding of E-safety issues amongst all member agencies.		
Schools & Youth Clubs competition Circulation of Strategy to all partner agencies Development of Policy template. Request key contact for each agency. Agencies to take Strategy to their own Safeguarding Executives	Mar 09 Feb 09 Feb 09 Mar 09 Dec 09	AF YO
4 Enable all member agencies to respond to the risks posed to children and young people by their use of ICT		
Fund CEOP Ambassador Training for lead contact.	May 2009	YO
5 Improve safe access to the internet for children and young people		
Communication & Awareness Raising	ongoing	All
6 Monitor e-safety arrangements in Bromley		
BSCB conduct audit and monitor e-safety incidents	October 2010	E safety Task grp

Annex 1: Glossary of Terms and Acronyms used in the document

Becta	Becta leads the national drive to implement the Harnessing Technology Agenda
BSCB	Bromley Safeguarding Children Board
CAF	Common Assessment Framework
CAIT	Metropolitan Police Child Abuse Investigation Team
CEOP	Child Exploitation and On-Line Protection
CYPP	Children and Young Peoples' Plan
DCSF	Department for Children Schools and Families
ECM	Every Child Matters
HMI	Her Majesty's Inspector
ICT	Information and Communication Technologies
IDEAR	Individual Education Attainment Records (core of central pupil database)
LGfL	London Grid for Learning
LSCB	Local Safety of Children's Board
MIS	Management Information System
MLE	Managed Learning Environment – a type of Learning Platform
OFSTED	Office for Standards in Education
PCT	Primary Care Trust

Annex 2: Key drivers

Working Together to Safeguard Children 2006,

'The range of child abuse definitions and concepts are now being seen in an ICT environment'.
LSCBs responsibility

Every Child Matters – Staying Safe

The death of Victoria Climbié exposed shameful failings in our ability to protect the most vulnerable children. On twelve occasions, over ten months, chances to save Victoria's life were not taken. Social services, the police and the NHS failed, as Lord Laming's report into Victoria's death made clear, to do the basic things well to protect her.

Children's and Young People's Plan

Staying Safe Action Plan

Byron Review

DCSF/Becta recommendations (Safeguarding Children in a Digital World)
Pan-London Child Protection Procedures

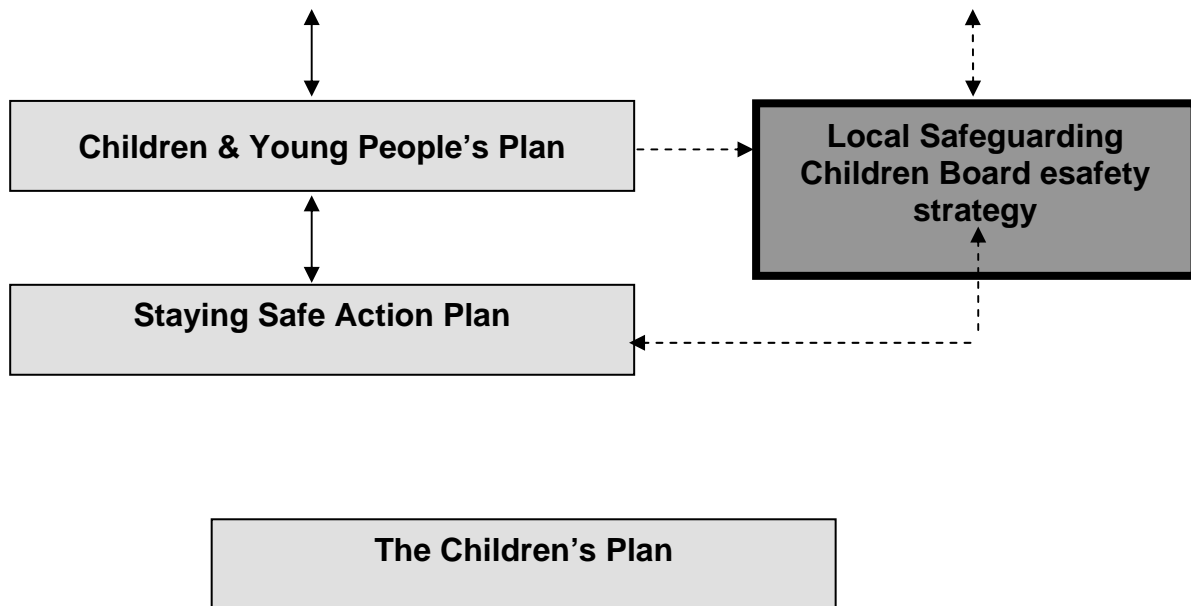
The Children's Plan – Building Brighter Futures

The Children's plan aims to make England the best place in the world for children and young people to grow up.

Annex 3: Interdependencies

This document sets out the relationship between the BSCB e-Safety Strategy and other local plans and strategies.

- BSCB Strategic Plan & Business Plan
- BSCB Communication Strategy
- LBB Children and Young People’s Plan
- LBB Positive Behaviour Strategy (Anti-Bullying)



Annex 4 Example Network Account Agreement – Student

FACILITIES

The _____ network allows you to save work in a protected area on the network, use printing facilities, access the Internet and use email for _____ work.

_____ has a policy which encompasses a whole _____ awareness of the problems of misuse of the I.T. system concerning intimidation, prejudice, exploitation and bullying or harassment of any kind.

_____ will use all technological tools and systems available to respond to any misuse and its effects to seek out and preserve evidence, to be used in the disciplinary process whether internal or for use by external enforcement agencies.

All children and young people who feel that they are victims of the misuse of the I.T. systems should contact _____ E-Safety Co-ordinator, on _____ all calls will be treated in confidence.

By agreeing to this use policy, you agree and understand the following conditions.

YOUR RESPONSIBILITIES

- DO keep your password safe and secure – you are responsible for any and all activity.
- DO remember to logout when you have finished your session.
- DO leave the workstation area as you would expect to find it.
- DO NOT give your password to anyone – even a friend.
- DO NOT attempt to access areas of the network you know you are not authorised to use
- DO NOT connect a home laptop, or other network device to the network.
- DO NOT attempt to logon as someone else (this is classed as hacking).
- DO NOT attempt to take control of another users' computer (this is classed as hacking).
- DO NOT attempt to disrupt the running of the network.
- DO NOT use chat rooms, instant messaging or attempt to watch live internet broadcasts.
- DO NOT attempt to download or install software/programmes onto the computers.
- DO NOT use the computers to download illegal music, videos or explicit material.
- DO NOT send any material which might cause offence via any medium (e-mail, podcast, messaging vodcast, smart phone etc.) to anyone from the college system or other web based systems.
- DO NOT send (inappropriate e-mails sent to large amounts of users).
- DO NOT plug any unauthorised devices into the _____ network (this includes PDAs, Laptops etc).

WHAT HAPPENS IF I BREAK THE AGREEMENT

_____ will monitor your work activity on the network. If you misuse any of these facilities you will receive a warning*, and depending on the seriousness of the incident, your access may be limited or removed. And you may be suspended from the _____.

*Warnings

YELLOW– Serious Concern Notice: Account Suspended for 2 days, tutor informed & letter sent home (if under 18).

RED– Final Concern Notice: Suspension of account for 2 days, tutor and Student Services Manager informed, contact made with parent/guardian (if under 18).

BLUE– Gross Misconduct Note – Immediate with Student Services Manager, probably suspension from College and police notified if offence is of unlawful nature.

PROTECTING OF SYSTEMS

In order to protect all children and young people who use this service, all Internet access, email transmission and computer use is audited and can be monitored by Senior Staff. If necessary this information can be used as evidence of misuse and may lead to your exclusion from _____ or given to the police if requested.

A copy of the information held in audit logs is available from the IT team upon request in order to comply with the freedom of information and Data Protection Acts.

Orpington College Updated: March 2008

Annex 5 Example Network Account Agreement (Staff)

FACILITIES

The _____ network allows you to save work in a protected area on the network, use printing facilities, access the Internet and use email for _____ (and a reasonable amount of personal work).

_____ has a policy which encompasses a whole organisation awareness of the problems of misuse of the I.T. system concerning intimidation, prejudice, and bullying or harassment of any kind.

_____ will use all technological tools and systems available to respond to any misuse and its effects to seek out and preserve evidence, to be used in the disciplinary process whether internal or for use by external enforcement agencies.

All staff who feel that they are victims of the misuse of the I.T. systems should contact the E Safety Co-ordinator: _____ on _____ all calls will be treated in confidence.

By agreeing to this use policy, you agree and understand the following conditions.

YOUR RESPONSIBILITIES

- DO Keep your password safe and secure – you are responsible for any and all activity.
- DO remember to logout when you have finished your session.
- DO leave the workstation area as you would expect to find it.
- DO NOT give your password to anyone – even a friend or colleague.
- DO NOT attempt to access areas of the network you know you are not authorised to use.
- DO NOT attempt to logon as someone else (this is classed as hacking).
- DO NOT attempt to disrupt the running of the network.
- DO NOT use chat rooms, internet messaging or attempt to watch inappropriate internet broadcasts or inappropriate web sites.
- DO NOT attempt to download illegal, unlicensed or inappropriate software or programmes onto the computers.
- DO NOT install software or programmes onto computers unless authorised to do so by SMT. All such software must have suitable licenses.
- DO NOT use the computers to download illegal music, illegal or explicit videos or any other illegal or explicit material.
- DO NOT send any material which might cause offence via any medium (e-mail, podcast, messaging, vodcast, smart phone etc.) to anyone from the college system or other web based systems.

PROTECTING OF SYSTEMS

In order to protect all children, young people and staff of _____, all Internet access, email transmission and computer use is audited and can be monitored by Senior Staff. If necessary this information can be used as evidence of misuse and may be passed to your line manager.

A copy of the information held in audit logs is available from the IT team upon request in order to comply with the freedom of information and Data Protection Acts.

Definitions:

Inappropriate – in this context meaning a web site, video, programme, software or material that cannot be reasonably justified for the purposes of education and teaching. It is recognised that an inappropriate web site may be justified for some specific courses/teaching needs.

Appropriate - Having sufficient or the required properties for a certain purpose or task; appropriate to a certain occasion.

Orpington College Updated: January 2009

Annex 6: E-Safety Audit Template

Bromley Safeguarding Children Board expects its partner agencies to audit regularly the e-safety arrangements in relation to safeguarding children within its relevant organisations. The audit forms part of the Board's E-Safety Strategy which recognises that children are citizens of a digital world and that we have a duty to safeguard and promote the welfare of children. **Please return forms to your safeguarding lead agency or to the BSCB (see address below) by**

Name of organisation: _____

Has the organisation got an e-safety policy, or integrated e-safety into its Safeguarding Children Policy?	Y/N
Date of the latest update to the policy (recommended annual)	
The policy has been publicised to staff?	Y/N
The policy is available to staff?	Y/N
The policy has been publicised to parents, carers, young people and children.	Y/N
Responsible manager for e-safety is:	
Responsible Trustee/ Board member/Governor is:	
Designated child protection/safeguarding is:	
Has there been specific e-safety training for staff?	Y/N
Has there been specific e-safety education for service users?	Y/N
Is there a clear procedure for responding to incidents or concerns?	Y/N
Is this procedure part of your overall safeguarding procedure?	Y/N
Have e-safety materials and information been obtained from CEOP, BECTA, ChildNet International or other source?	Y/N
Is there an Acceptable Use Policy in Place?	Y/N
Do all your staff and volunteers sign a Code of Conduct/Acceptable Use Agreement on appointment?	Y/N
Are all your service users aware of your Acceptable use Policy?	Y/N
Are e-safety rules clearly displayed in all places where digital technology is used and expressed in a form that is accessible to all service users?	Y/N
Are children and young people taught about safe use of digital technology?	Y/N
Do children and young people know who to report e-safety concerns to?	Y/N
Do parents/carers and young people over the age of 16 sign and return an agreement that their children will comply with the organisation AUP?	Y/N
Is internet use and the network monitored?	Y/N
Can individual use been traced?	Y/N
Are staff, volunteers and service users aware that network and internet use are monitored?	Y/N
Is personal data collected, stored and used according to the Data Protection Act?	Y/N

Annex 7: Membership & Governance

LSCB Membership

Bromley MyTime

Bromley Primary Care Trusts (PCT)

Bromley Hospitals Trust

CAFCASS

South London and Maudsley NHS Trust

LBB – Children and Young People Department

LBB – Adult and Community Services

London Probation

CAIT

Borough Police

BSCB Sub-committees

Main Board

Executive Committee

Education Sub Committee

Health Sub Committee

Policy, Procedures and Communication Sub Committee

Quality Standards Sub Committee

Training