EALING SAFEGUARDING CHILDREN BOARD

E-Safety Strategy

Safeguarding Children & Young People in a Digital World

'New technologies are integral to the lives of all children, young people and their parents. They inspire children to be creative, communicate and learn. It is essential that children and young people tap into the potential of the digital world if they are to enjoy their childhood and succeed in life. In educating children and young people we should empower them to learn how to use digital technology responsibly, not simply block what they can access. We must give them the information and skills they need to be digitally literate and savvy users. This enables them to take advantage of the opportunities that new technologies can offer, as well as being able to deal with any risks that arise'.
Dr Tanya Byron March 2010

What does e-Safety mean?

The rapid growth of the internet and availability of a wide range of digital/mobile technologies accessible to all is both exciting and challenging. Like anything else in life whilst benefiting from the learning and communication opportunities the issues and risks must be properly assessed. Children and young people must to be protected from risks where possible and need to be educated and supported to develop the skills to keep themselves safe when using technology. Similarly adults with a duty of care to safeguard children and young people must be properly informed about this subject.

Under the Children Act 2004 (s11) and the Education Act 2002 (s175/s157) all professionals have a duty to safeguard and promote the wellbeing of all children. The duty of care to protect young children cannot be confined to a single environment but must extend to all environments in which young people actively engage whether this is school, home, or the wider community. This requires an integrated approach across schools and other establishments that regularly come into contact with young people. Ealing Safeguarding Children Board (ESCB) will take the responsibility for seeking assurance from all of Ealing's agencies and partners that e-safety is adopted as a priority.

Ealing's Strategic Aim

ESCB wishes to encourage and develop the safe use of digital and mobile technologies through the education not only of children and young people but also the adults who have a duty of care for them.

This key aim is part of the ESCB's e-safety responsibilities and requires the Board and its member agencies and partners to work together in a pan-Ealing approach. This approach will seek members' and partners' assurance that adults and children within their area know how to act responsibly and how to benefit from the effective and safe use of digital and mobile technologies both now and as they emerge.

This includes:

- every child and young person
- every professional, practitioner and volunteer with a duty of care for children and young people
- every parent/carer and family
- specific groups, such as vulnerable children and young people, and also vulnerable adults

Who does this Strategy apply to?

It applies to everyone in Ealing's community. There are a broad range of agencies and services who contribute to the safeguarding of all members of Ealing's community.

They include ECSB member agencies and community groups.

ESCB member agencies

Children's Social Care	Ealing Primary Care Trust
LBE Schools Service	Ealing Community Health Services
LBE Early Years	Ealing Hospital Trust
Youth Offending Service	West London Mental Health Trust
LBE Adults' Services	Central & NW London NHS Foundation Trust
LBE Housing	ESCAN
CAFCASS	Ealing borough police
Ealing Preschool Learning Alliance	Met police CAIT
Hestia Housing	Ealing Probation
Youth and Connexions	

What are we Safeguarding against?

If we can encourage positive and responsible behaviours when using the internet or any digital and mobile technologies we go a long way to safeguarding everyone. Understanding the risk categories associated with behaviours helps us to identify key issues and risks which then in turn allows us to take positive action.

	Commercial	Aggressive	Sexual	Values
Content (child as recipient)	Adverts Spam Sponsorship Personal info	Violent/hateful content	Pornographic or unwelcome sexual content	Bias Racist Misleading info or advice
Contact (child as participant)	Tracking Harvesting personal info	Being bullied, harassed or stalked	Meeting strangers Being groomed	Self-harm Unwelcome persuasions
Conduct (child as actor)	Illegal downloading Hacking Gambling Financial scams Terrorism	Bullying or harassing another	Creating and uploading inappropriate material	Providing misleading info/advice

Ref*: In 'The Report of the Byron Review', Dr. Byron refers to this classification of e-safety risk (as structured by the EU Kids Online Project in 2007)*

Children and young people can have access to the internet anywhere and at any time with mobile technology. The age at which children are carrying mobile phones is getting younger all the time. It is therefore the understanding of what risks there are with any digital technologies that helps us to provide a means of managing and mitigating these.

Content, Contact and Conduct are now considered to be the recognised terms when expressing risk groupings associated with e-safety. Although the grid has been defined in terms of 'child' use, it is just as relevant to everyone who uses digital and mobile technologies.

Content: eg, where the child/person unintentionally has access to content that is inappropriate and where perhaps using a search engine returns information that is misleading

Contact: eg, where the child/person is unwittingly a participant in perhaps a chat room, being persuaded to give out personal information and opening up the opportunity for being bullied or groomed

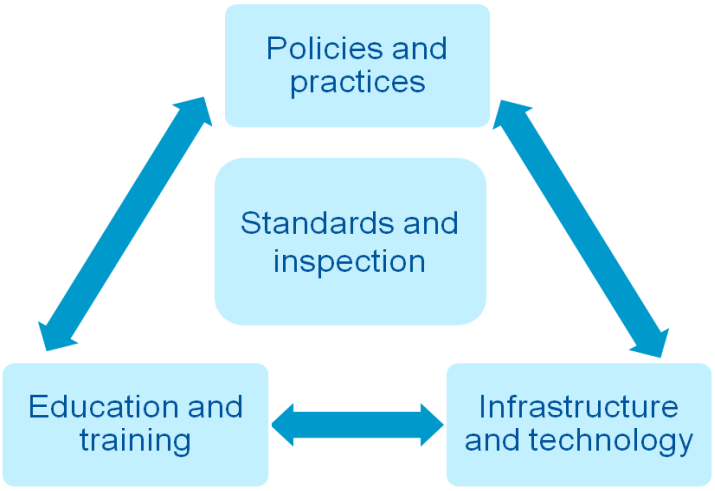
Conduct: eg, where the child/person is behaving inappropriately online, or being the instigator of bullying, pretending to be someone else, or illegally downloading and sharing files

How do we manage e-Safety Risks and Issues?

'Children and young people need to be empowered to keep themselves safe – this isn't just about a top-down approach. Children will be children – pushing boundaries and taking risks. At a public swimming pool we have gates, put up signs, have lifeguards and shallow ends, but we also teach children how to swim.'
Dr. Tanya Byron
Safer Children in a Digital World: The Report of the Byron Review

By adopting a nationally accepted best practice model (PIES), we can tackle the types of issues and risks identified above.

The PIES Model



The PIES Model , Policies, procedures, practices
Policies must be updated and/or created to specify the responsible use of digital and mobile technologies. Acceptable Use Policies (AUPs) are specific agreements between parties which ensure there is commitment and understanding on both sides as to the roles and responsibilities (governance) towards e-safety. Policies are translated into procedures and practices, and these need to reflect accurately what the policies are saying and also be enforceable and practical in their use.

The PIES Model , Infrastructure – the technical provision of protection

There is a level of technical protection that can and should be implemented in any given institutional environment. This is the area that relates to email and content filtering, website blocking, black and white word lists, spam and virus control, authentication, monitoring systems and so on. The success and robustness of any infrastructure is only as good as the policies and behaviours that go with it.

The PIES Model , Education, awareness, training

There can be secure and safe infrastructures and meaningful policies and procedures, but by far the greater weight of this PIES triangular model is the attention to raising awareness, education and training on what benefits the internet holds for children and young people as well as the risks they might need to manage. Professionals, practitioners, volunteers, parents, carers and children and young people all need to understand the importance of safe and effective online behaviour.

The PIES Model , Standards, monitoring, performance, inspection

At the end of the day there is a continual need for assessment, to see if policies are working, if the training has been effective and whether the action plans to support an e-safety strategy have been successful. The digital world does not stand still and there is an increasing need to be continually updating, monitoring and checking.

Ealing's Strategic Objectives

In order to assure ESCB that e-safety is being positively managed the following key objectives have been set:

<u>Policies, Procedures and Practices</u>

- For the ESCB to be assured that all members of Ealing's community (please refer to the diagram on page 3) whether a provider or a setting, have in place policies, procedures and practices that enable those with a duty of care to safeguard children and young people, as well as children and young people themselves to use the internet, digital and mobile technologies safely and responsibly.

<u>Infrastructure and Technology</u>

- For the ESCB to be assured that that those responsible for the key infrastructures providing internet service and management across Ealing's community both for the workforce and for children and young people will ensure that they are fit for purpose, up to date, secure and safe.

Education, Training and Information

- For the ESCB to be assured that all members of Ealing's community (please refer to the diagram on page 3) whether a provider or a setting, have in place the necessary training and awareness programmes that enable those with a duty of care to safeguard children and young people, as well as children and young people themselves to use the internet, digital and mobile technologies safely and responsibly.
- For the ESCB to be assured that guidance, good practice and information is freely available and accessible to all citizens.

Standards, Inspection and Monitoring

- For the ESCB to be assured that the management of incidents relating to e-safety can be embedded in a consistent way as part of the safeguarding responsibilities of member agencies and partners of the ESCB (to include incident identification either directly as an e-safety issue or as part of existing child protection, reporting using common monitoring datasets and referral).
- For the ESCB to be assured that there is ongoing consultation with children and young people about their concerns and needs regarding their use of digital and mobile technologies and that this informs policies, education and incident management.

Implementation ,Ownership and Accountability

This Strategy on e-safety has been produced following consultation and analysis of good practice by representative agencies and partners of Ealing Safeguarding Children Board (ESCB). It is an over-arching strategy for all of Children's Services, agencies and partners in Ealing, and can be used to base individual e-safety strategies on if required.

Following adoption of the strategy by the ECSB all partner agencies will be asked to review their e-safety practice and develop their proposed action plan. The review will be conducted using an audit framework based on the 4 key strategic objectives. (Framework attached at appendix one below) Sources of support and training will be made available to agencies as part of the audit system.
:

Through the workplan of the Performance & Quality Assurance Subgroup the ECSB will monitor and support services's adoption of the key objectives , their conduct of an audit , and their development of an action plan based on the audit.

Appendix one

Ealing E-Safety

Audit of Progress against Key e-Safety Objectives by Agencies/Partners

The following actions are related to the Strategic Key Objectives in the Ealing (ESCB) e-Safety Strategy. This audit is to assess the progress against these Objectives so an action plan can be developed to ensure the key E-Safety objectives are fully met.

Key Objective	Action
Policies, Procedures & Practices For the ESCB to be assured that all members of Ealing's community whether a provider or a setting, have in place policies, procedures and practices that enable those with a duty of care to safeguard children and young people, as well as children and young people themselves to use the internet, digital and mobile technologies safely and responsibly.	Please respond to the following questions on whether your agency/organisation has any policies, procedures, practices in place regarding e-safety, eg use of mobile phones, AUPs (Acceptable Use Policies), dealing with cyberbullying, etc. Please note that e-safety does not necessarily require specific additional policies to be in place and that addition/amendment may be sufficient. *1. Has your agency/organisation:* a) Identified which policies need amending? (yes/no – if yes please state which ones) b) Made the relevant changes? (yes/no – if yes please give examples of changes) c) Needed to create new policies (yes/no – if yes please state which ones) **Please state if your agency/organisation requires assistance with their policy review.**
Infrastructure & Technology For the ESCB to be assured that that those responsible for the key infrastructures providing internet service and management across Ealing's community both for the workforce and for children and young people will ensure that they are fit for purpose, up to date, secure and	*2. Please respond to the following questions on whether your agency/organisation knows:* a) Who provides their internet service provision? (yes/no – if yes please state who it is and if their policies and protocols are available for review if required?) b) Who to refer to for information and guidance about emerging technologies, their benefits and risks? (yes/no – if yes please identify who this is) **Please state if your agency/organisation requires assistance with understanding and identifying their internet service provision and management.**

safe.	
Education & Training For the ESCB to be assured that all members of Ealing's community whether a provider or a setting, have in place the necessary training and awareness programmes that enable those with a duty of care to safeguard children and young people, as well as children and young people themselves to use the internet, digital and mobile technologies safely and responsibly.	Please respond to the following questions on what your agency/organisation is doing with regarding to e-safety training, education and awareness raising: 3. *Has your agency/organisation:* a) Identified the training needs of all of your staff members and users (eg school staff, students, parents, governors) including volunteers? (yes/no – if yes please give a summary of requirements) b) Identified training content and providers? (yes/no – if yes please give a summary of content and a list of providers) c) Commenced a program of training? (yes/no – if yes please give a summary) d) Collected outputs/feedback? (yes/no – if yes please give an estimate of how many have been trained and how successful the training has been) e) Embedded training, education and awareness raising? (yes/no – if yes please summarise) **Please state if your agency/organisation requires assistance with any aspect of training, education and awareness raising.**
For the ESCB to be assured that guidance, good practice and information is freely available and accessible to all citizens.	*4. Has your agency/organisation:* a) Considered how e-safety information, advice and guidance might be disseminated to the wider public? (yes/no – if yes please give details) b) Considered working with other agencies/organisations to raise the profile of e-safety generally? (yes/no – if yes please give details) **Please state if your agency/organisation requires assistance with the dissemination of information to the wider public,**
Standards, Inspecting & Monitoring For the ESCB to be assured that the management of incidents relating to e-safety can be embedded in a consistent way as part of the safeguarding responsibilities of member	Please respond to the following questions on what your agency/organisation is doing about incorporating e-safety in their incident management procedures: *5. Does your agency/organisation:* a) Have an e-safety incident management system? (yes/no – if yes please provide a copy) b) Identify e-safety aspects in child protection incidents? (yes/no – if yes please explain how this is done?

agencies and partners of the ESCB (to include incident identification either directly as an e-safety issue or as part of existing child protection, reporting using common monitoring datasets and referral).	c) Identify e-safety aspects in adult allegation cases? (yes/no – if yes please explain how this is done? **Please state if your agency/organisation requires assistance with considering what constitutes an e-safety incident and how e-safety might form part of its incident management system.**
For the ESCB to be assured that there is ongoing consultation with children and young people about their concerns and needs regarding their use of digital and mobile technologies and that this informs policies, education and incident management.	Please respond to the following questions on what your agency/organisation is doing about consulting with children and young people: *6. Does your agency/organisation:* a) Conduct any surveys or questionnaires? (yes/no – if yes please give details of what and how often) b) Use the information to inform policies and education programmes? (yes/no – if yes please state how) c) Share the information with other agencies/organisations? (yes/no – if yes please state which ones) **Please state if your agency/organisation requires assistance with conducting consultation.**