Managing E-Safety and Strategy

Contents

1) Introduction

This policy provides guidance, in accordance with the effective approaches to e-safety within the LBH and more specifically, Westbrook Short Break Unit. The overarching focus of this document is to not only ensure that pre-existing policies are being applied, as and when needed, with regards to digital emersion and online environments. This policy will be scrutinised thoroughly and revised within junction to any new or reviewed policies, should it be deemed necessary.

2) Background

E-safety encompasses the use of technologies (both fixed and mobile) that a child or young person may encounter at some point in their life. These devices further communication, as well as accessing

content on alternative platforms. This opportunity, while managing to be educational, social and sometimes sensory, poses issues and/or risks to the wellbeing of the designated child or young person that is accessing these technological mediums.

Within Staff's line of duty, safeguarding children and young people is paramount; this encompassing e-safety. This role does not fall to a specific member of the team, but rather to be considered as part of the overall safeguarding arrangements in place, protecting the welfare of all service users.

Both staff and service users alike can benefit from correct e-safety practice. E-safety itself relates to any communication on the internet, suitability of content, use of social media, mobile devices and other electronic communication means, and how in which they pose a threat to the well-being or safety of an individual.

While technological advancement is a key, having skills integrated into both work/School practice and social contexts, the underlying threat of safety being breached is something both staff and services users should be aware of. As ICT skills are proving to be more and more essential, it is important we have a working understanding of the risks we may come across and how to effectively manage the situation, as well as being able to build on the ICT skills we may already hold, encouraging the positive impact that may stem from the internet/ technological interfaces.

To effectively manage this potential risk, it is essential that we not only include the Children and Young People in this body of work, but also their parents and/or carers. This would not only widen the "bubble of safety" that we create at Westbrook, but helps to educate the wider community further into protecting themselves and the children in their care, with regards to online technologies.

It is paramount that all staff working with the Children and Young People are familiar, clear and confident with safe practice. This not only relates to the safety of the services users, but to further the protection of staff against misunderstandings, and allegations of inappropriate behaviour. i.e. 1) Never signing a service user onto an account with your details such as YouTube or Facebook. 2) Sending correspondence via a school e-mail, regarding homework, and not to a personal e-mail.

While risks can be diminished as best as possible, it is not feasible to create a 100% safe environment while exploring online. At Westbrook, it is our responsibility to demonstrate/ evidence where, and how, we have minimised or eradicated potential threat to the utmost of our ability. Any incidents that may occur should be logged swiftly, so that the issue can be effectively resolved/followed up.

It is important that we can instil a sense of sagaciousness into the Children and Young People, helping them filter out irrelevant or wrong information. It is easy for many people, in all walks of life, to misjudge information published online. An article or framework published online has no correlation to the merit of its truth, thus, staff and services users alike must be able to filter this information, selecting only the relevant and true. Developing the skills to be able to select and evaluate internet-based information, is just as important as the recording, and filtering information from other means, such as newspapers, radio and TV. We can further this skill by using our own judgement to determine the facts, the fiction and the opinions that may lay within a frame of information, questioning deeper the plausibility and/or biases.

In addition to accessing the internet via Westbrook (or any other means of supervision), Children and Young People will have independent time on the internet or be immersed in other digital technologies. This is when the highest level of risk may occur, hence the importance of instilling the

ideals of internet safety into the service users as much/often as possible. While a Child or Young Person should be supported where and when needed, it is important their online confidence grows, and their ability to access the digital world should flourish, they should have awareness of danger and how to respond accordingly.

3) The Risk

It is essential as staff that we understand, the scope of risk to Children and Young People, whilst divulged into a cybernetic environment, is vast and ever-changing. The table below references "The Byron Report" 2008, (reviewed 2018) – highlighting the risks posed, from different perspectives, mediums and/or roles played.

	Commercial	Aggressive	Sexual	Values
Content (Child as recipient)	• Adverts • Spam • Sponsorship • Personal Information	• Violent/Hateful Content	• Pornographic or unwanted sexual content	• Bias • Racism • Misleading information or Advice
Contact (Child as participant)	• Tracking • Harvesting personal information	• Being Bullied, Harassed or Stalked	• Meeting Strangers • Being Groomed	• Self-Harm • Unwelcome persuasion
Conduct (Child as Acter/Perpetrator)	• Illegal Downloading • Hacking • Gambling • Financial Scams • Terrorism	• Bullying or Harassing Another	• Creating and Uploading Inappropriate Material	• Providing Misleading Information or Advice

Aside from the risks that may pose a threat due to the content of material, risks regarding Children and Young Person's well-being may also exist in a number of ways.

It is known that adults who want to abuse or exploit children online use fake/decoy accounts, normally posing as children or young adults to engage a child or young person in communication, usually resulting with/aiming to meet them. This is known as "grooming" – an act whereby an adult prepares a child or young person to be abused in any respect. This is usually a slow process, using forums such as chat rooms and social media platforms over a long period of time to build trust and rapport with the participant, making it harder for the victim to speak out or question.

Cyberbullying is ever-growing and become more prevalent in the 21st century. Bullying takes many forms online and occurs daily – a small selection if these types of bullying include sending threats

online, abusive texts/instant messages, posting insulting comments about people on social media or other platforms (e.g. Twitter, Facebook and other various Blogs), sharing embarrassing or derogatory pictures and/or videos of an individual. While online bullying is easy and the added anonymity allows people to feel free in their expressions, most cyberbullying is accompanied by face-to-face or other physical bullying, and should not always be treated as a standalone case.

Sexual (and criminal) exploitation may arise in situations where and individual has allowed images or videos to be captured of themselves in provocative or compromising circumstances. Not only is it a risk that these images may be uploaded or circulated on certain platforms, it is more than likely that people with these images can use them to coerce individuals to perform tasks/favours in order to keep these images concealed. Moreover, the victim could become subject to blackmail and be extorted for goods, money and/or services. This category of exploitation is not restricted to elders online only. It has been recorded that young people i.e. gang leaders, have used these methods to entice younger people to join or work for their gang. In some certain examples, the victim may be gifted expensive or unattainable items they desire, making them feel indebted to/ entrusting to someone who is grooming them.

4) E-Safety policy

The subcategories below identify and highlight the requirements within Westbrook to maximise the safety of the Children and Young People that access the service.

4a) Acceptable Use Policy (AUPs)

As Westbrook has services users who can and do access the internet, it is imperative we have our AUP's in place, helping set the guidance for acceptable, safe and responsible internet use. The AUP's should not only ensure the safety of the children and young people, but the adults who work within this setting. Appropriate variations of the AUP's should be available for all audiences and cognition levels.

Children and Young People

- Age and cognitive understanding levels should be considered when shown the AUP's.
- Service users should be made aware of all and any updates to the AUP's.
- Parents/carers should have access to any policies put into place.
- AUP's should be included in the staff induction process to drive home the importance of these policies.

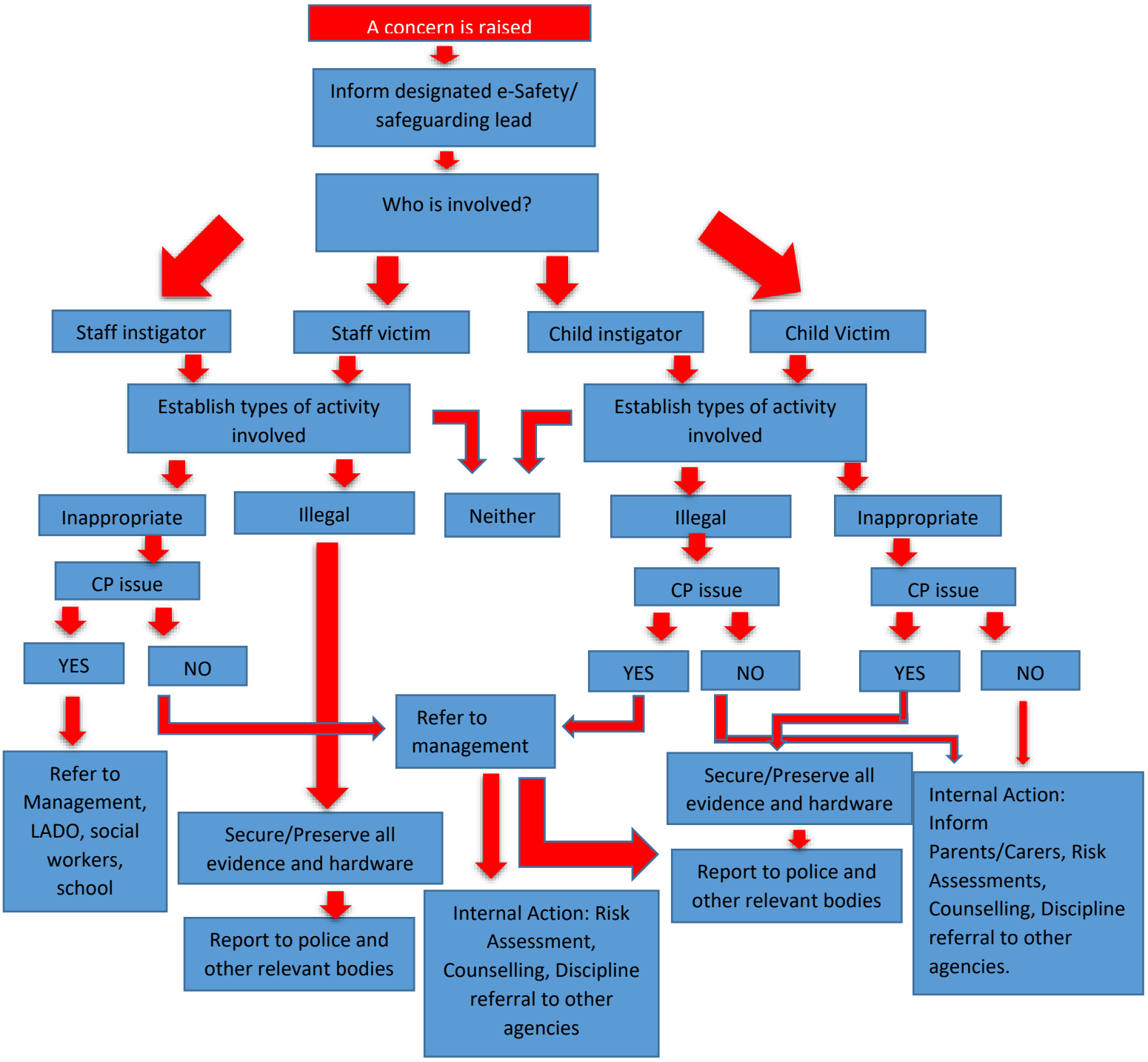
4b) e-Safety Lead

It is within the best interest of Westbrook to have a lead e-Safety person (normally management and safeguarding lead) who can champion the responsibility of internet awareness and safety, including;

- Maintaining or Updating the AUP's
- Ensuring that the Westbrook Policies folder references aspects of e-safety i.e. bullying policy should have a cyberbullying clause.
- Implementing and monitoring the effeteness of child safety filters, and what level they operate at
- Reporting any bugs or issues that may arise with software, inter/intranet
- Ensure staff have read the E-safety policies (on induction) and have had training on the matter
- Record and evaluate incidents that occur (helps develop quality of e-safety policies and frameworks)

4c) Managing Incidents

Follow the flow the chart accordingly, in reference to the management of incidents –



The management/e-safety and safeguarding lead must ensure all staff and relevant adults follow this flow chart in the events of someone misusing the internet, including;

- Inappropriate Contact
- Bullying
- Malicious comments or threats towards Children, Young People and Staff
- Viewing inappropriate content and/or Access restricted or illegal websites
- Allegations against Staff
- Whistleblowing process

5) Sexual exploitation, the internet and mobile phones

In 1988, the current legal framework regarding the exposure of child abuse related images was established. As technology advances and grows, unfortunately, so does the opportunity for children to be exploited or exposed to harmful imagery. Legal guardians, parents, carers, as well as professional bodies alike grow increasingly anxious around children using the internet as 1 in 5 young people who access social media or chatrooms are reported to be approached by a paedophile.

It is clear, in abundance, that children and young people must be educated correctly with regards to the internet, being able to realise and avoid the risks that they may encounter, or be able to convey this message to a responsible adult – Adults should be expected to supervise and protect children and young people as and when needed, when using or accessing the internet.

Children may use different devices to access different sites and content, thus, staff should be mindful of how and when the children and young people are using mobile devices or personal laptops, etc.

6) E-Safety group strategy

A three pronged approached in raising awareness will help with this;

- Understanding of e-safety amongst children and young people
- Understanding of e-safety amongst parents and carers
- Understanding of e-safety amongst all members of staff and any other professional working with children and young people

Internet safety becomes a shared, group responsibility. Children and Young People should be encouraged to develop their online skills and be taking on more responsibility for their actions. It is only through positive role modelling (both adults and peers) that this can happen, to help ensure the safety and well-being of the modern day child.

Westbrook also believe in the key role of staff, parents and carers monitoring and promoting the safe use of modern tech, as well as the ability to give advice and guidance to children or young people that may ask.

7) e-Safety Action Plan

1 – Raise awareness and understanding of e-safety issues amongst children and young people

Objective	Action
1A. Make e-safety a talking point for children and young people.	• A wide range of resources made available for all children and young people regarding the topic • At Westbrook, support is available to parents and carers with information they may need, for staff regarding their training and for any other relevant bodies • Inclusion of e-safety with regard to bullying • Linking with Safeguarding lead • Links to additional services in the LBH I.E. Youth clubs, Play team etc. as well as relevant school of service users
1B. Increase awareness of resources that support children to behave safely online.	• Working with relevant parties I.E. school as stated above • E-safety is something we talk about and develop in care plans and in our evidenced outcomes

2 – Raise awareness and understanding of e-safety issues amongst parents and carers

Objective	Action
2A. Improve levels of awareness amongst parents and carers of the risks posed to children and young people by their use of technology 2B. Improve levels of awareness of parents and carers of ways they could mitigate the risks posed to our service users 2C. Improve awareness amongst parents and carers of available resources in the area/online 2D. Increase awareness of how to respond to and report incidents when not at Westbrook	• Connective and joint work with families • Connective and joint work with placement teams • Raise awareness within other agencies that work in conjunction with Westbrook • Introduction and use of Intranets • Highlight the e-safety standards in our statement of purpose

3 – Raise awareness and understanding of e-safety issues amongst all agency workers

Objective	Action
3A. Increase the volume of professionals with an understanding of the importance of e-safety and how to deal with the issues 3B. To continue to raise the profile of e-safety amongst professionals and practitioners	• Ensure each employer/management is checking the skills and awareness levels of their staff and training them accordingly • Develop e-safety training to be available to all Westbrook staff with appendices and sources to read from

4 – To link with the work of LBH and their policies regarding e-safety

Objective	Action
4A. Increase awareness across all areas of e-safety, bully and child sexual exploitation	• Common cross over areas between these three groups • Hold common basic awareness training events that cover and diverge into these areas • Ensure all material and presentations refer to the other related areas and support each other with cross referencing • Alert and inform all relevant bodies needed if a child seems to be at risk. (see above flow chart is section 4C)

8) Information and Websites about e-safety

- Think U Know(information group by age and role i.e. child or parent) - https://www.thinkuknow.co.uk/
- Childnet (online safety activities and information) - https://www.childnet.com/
- UK Internet safety centre - https://www.saferinternet.org.uk/
- NSPCC e-Safety - https://www.nspcc.org.uk/keeping-children-safe/online-safety/
- Internet matters (Parents/Carers) - https://www.internetmatters.org/
- Childline (Bullying and e-safety) - https://www.childline.org.uk/info-advice/bullying-abuse-safety/online-mobile-safety/staying-safe-online/
- Hector the Protector (Downloadable program to help filter children's content online and helps if they do come across something inappropriate) - http://hectorsworld.netsafe.org.nz/teachers/hectors-world-safety-button/