PROCEDURES AND GUIDANCE

Online Safety

Date of original document	April 2016	
Date document reviewed	January 2018 July 2018 April 2021	
Date for next review	December 2021	

EAST RIDING SAFEGUARDING CHILDREN BOARD

Online Safety Procedures and Guidance

1   Introduction

1.1   The East Riding Safeguarding Children Partnership takes seriously its statutory role to ensure that all member agencies co-operate to safeguard and promote the welfare of children and young people in the East Riding of Yorkshire and to ensure that they are effective in doing so.

1.2   The rapid growth of the internet, social networking and of electronic technologies generally has opened up a new world of exciting opportunities for many children and young people. Through the internet and mobile technology it is possible for them to have access to almost unlimited information worldwide, to be entertained and, through social networking sites to contact and socialise with other young people. Alongside the benefits there are also significant risks, and whilst many children and young people are very competent in using such technologies, their knowledge, as well as their parents/carers of the risks should be strengthened.

1.3   The risks to children and young people are various but the East Riding Safeguarding Children Board is committed to ensuring that children and young people are kept safe from a range of dangers, including but not limited to:

- Sexual Exploitation
- Criminal Exploitation including County Lines
- Bullying, including cyber based or prejudiced based bullying
- Impact of technologies on sexual behaviour
- Radicalisation and Extremism
- Substance Misuse
- Self-Harm and Suicide
- Eating Disorders
- Online Gambling
- Online Gaming
- Modern day slavery/human trafficking

1.4   These procedures and guidance provide the Online Safety framework for member agencies of the ERSCP together with other partners and organisations to work with children and young people, together with their parents or carers, in order that they can be safe when online or using technologies.

1.5   Being safe online is not simply a matter of technology and, as such, the procedures and guidelines encourage a comprehensive approach to on line safety in which children and young people are kept safe by sound policies that inform technical standards. It sits alongside a programme of education which develops and sustains safe on line behaviour. This document will be monitored by the ERSCP to ensure that it remains relevant to its aims as information technology changes and evolves.

2   Strategic Aim

2.1   The implementation of these procedures and guidance, along with the over-arching strategy, will be monitored through the ERSCP Contextual Safeguarding Strategic Group.

3   Reporting Safeguarding Concerns

3.1   If professionals or members of the public are worried about a child or young person or think they might be at risk of harm, abuse or neglect they should contact the ERYC Children's Safeguarding Hub (SaPH) (01482) 395500 who will listen to the concern and decide what action needs to be taken.

3.2   Where concerns relate to allegations of harm by a professional, volunteer or foster carer to a child, a discussion should be held with the Local Authority Designated Officer (01482) 396996. There is a specific guidance document relating to allegations of abuse made against adults working with children and these can be accessed [here](#).

4   Agency Online Safety Policies

4.1   All online safety policies should have a foundation of agreed policies that direct all agencies, including the voluntary and community sector, parents/carers and children and young people in the use of the internet.

4.2   Policies should include:

- Acceptable use procedures, where applicable
- Internet filtering procedures
- Referral and reporting procedures through an incident flow chart
- Education and Training

4.4   These should be interpreted into online safety policies that can be applied to schools and all agencies who work directly with children and young people.

4.5   Access to the internet must be through equipment and connections that allow for a good level of protection, filtering, and professional/parental control accepting that this will be challenging when applying it to online devices. The strategy establishes what the standard will be and how agencies and individual families can enable this.

5   Acceptable Use and Behaviour Policies (AUP)

5.1   Acceptable Use Policies promote responsible use of the internet and online devices by ensuring that users are safe and not exposed to any damaging material and those systems are protected from accidental or deliberate misuse. They will apply to professional staff, volunteers, children and young people. AUP's will also cover all aspects of social networking which may include posts uploaded in the private lives of staff members but linked to information within the school or agency.

5.2   Agencies should;

- Twice yearly review and update their AUP
- Ensure that every user who works with children, young people and parents/carers, where applicable, are aware of the AUP, and accept and understand it.
- Ensure that professionals, volunteers, parents/carers and children and young people are aware of how to report and refer incidents.
- Provide advice and guidance to parents/carers on how to protect their child at home and in the community.

5.3   In addition to Acceptable Use Policies which focus on responsible use of the internet and online devices, Acceptable Behaviour Policies apply where there are concerns relating to inappropriate relationships between those who work with children and adults as outlined in the Sexual Offences Act 2003, namely:

- Having a sexual relationship with a child under 18 if the adult is in a position of trust in respect of that child, even if the relationship is said to be consensual (Sections 16-19, Sexual Offences Act 2003);
- 'Grooming', i.e. meeting a child under 16 with intent to commit a relevant offence (Section 15, Sexual Offences Act 2003);
- Other 'grooming' behaviour giving rise to concerns of a broader child protection nature (e.g. inappropriate text/email messages or images, gifts, socialising, use of social media etc);
- Possession of indecent images of children or use of the internet to access indecent images of children)

6   Filtering and Parental Controls

6.1   Internet providers in the UK, such as KCom, BT, Sky, TalkTalk and Virgin Media - provide their customers with free parental controls which can be activated at any time. They also provide helpful video guides to assist in downloading and setting-up the controls offered by the provider. Staff are available to give advice to help parents and carers, including children and young people, to access this support and become familiar with changes in settings.

6.2   We know that children, particularly younger children, can be bothered by things they see online, and filters can be a helpful tool in reducing the chances of coming across something upsetting. It should be remembered that filtering is only part of the solution.

6.3   The internet has become a key learning tool for schools, it is therefore important to provide right balance between providing a web filtering solution which helps to protect, but that still gives freedom to work without limits. The Councils schools filtering system provides different categories of access for pupils (including different levels for different key stages), staff and administrators. The system also allows for instantaneous blocking and unblocking of sites from the school premise without affecting the core white and black listed filtering.

6.4   No filter or parental control tool is 100% effective, and many of the risks that children and young people face online are because of their own and other's behaviour. It is therefore important to talk to children and young people about staying safe online and making sure they know that they can turn to a safe adult if they get into any difficulty.

6.5   Other services that are popular with children and young people also provide tools that are helpful to activate in addition to filters. Find out more about YouTube Safety Mode, Google SafeSearch, 4OD Parental Control, BBC iPlayer Parental Guidance Lock, ITV Player PIN number protection and Sky Go Parental Controls.

Devices that connect to your home internet

6.6   In addition to content filtering offered by an Internet Service Provider, many devices such as games consoles, smartphones and tablets have their own parental controls, for example to limit spending or restrict access to apps based on age rating. Likewise, many web browsers have built-in tools and features to help control the kinds of content users can view.

Staying safe when out and about

6.7   If children and young people are taking their devices out of the home, it is worth bearing in mind that they could connect to public WiFi, for example, in a shop, cafe or restaurant. Look out for the Friendly WiFi symbol which shows that the WiFi has filters in place to limit access to pornographic content.

7   Education and Training

7.1   Technical measures alone will not keep children and young people safe. There should be comprehensive education and training for professionals, volunteers, parents/carers, and children and young people to learn about the risks of the internet and the behaviours that are needed to stay safe online.

7.2   Online Safety in Schools and Colleges
Online safety is an important part of the curriculum for children and young people from early years through to Key Stage 5. In all schools and colleges internet safety should be embedded into the Computing curriculum. The DfE provides a framework to equip children and young people for digital life – Education for a Connected World which should be incorporates into the internet safety from Early Years to 18 years of age. In addition, online safety is taught in schools through Personal Social Health Education (PSHE), Sex and Relationship Education (SRE) and Citizenship lessons. The East Riding Prevention and Education Team offer bespoke training for students as well as training events for parents and carers. Online safety is also a theme for school assemblies.

7.3   While it is important that services and agencies ensure their staff undertake the relevant up-to-date training in terms of online safety, the onus is also on ensuring that parents/carers and children/young people themselves are aware of the current issues, resources and support available in terms of staying safe online. Professionals and volunteers should therefore ensure they promote this approach to the parents/carers and children/young people they support. Although not intended to be exhaustive, the ERSCP website does contain links to some of these resources, and can be accessed here:
http://www.ERSCP.org.uk

7.4   ERSCP Online Safety Training
The Online Safety training programme, run by the ERSCP, includes CEOP and ThinkUKnow information, and is a crucial element of the Partnership's Multi Agency Training Programme. Everyone working with children and young people and parents/carers should attend it, or an equivalent training programme. Online safety training should also be included in generic safeguarding training delivered by ERSCP member agencies to their own staff with appropriate signposting to more specialists training.

7.5   The ERSCP Multi-Agency Training programme can be accessed here:
http://www.ERSCP.org.uk/training/

7.6   The National Crime Agency's CEOP (Child Exploitation and Online Protection) website can be accessed here: http://ceop.police.uk/

Review Date: April 2021
Next review: December 2022