Background

The rise of easy-to-use, relatively inexpensive technology has been immense. There is more of it about these days than ever before, and it's only going to increase.

Children engage with it easily, and in many cases, far more easily than parents and carers. It is common to find adults saying that their children understand it better than they do.

Over the past year or so, we have seen more and more of this technology being installed in bedrooms and other private areas of the home where parents/carers do not have sight of what their children are doing.

This guide aims to help parents and carers create as much of an e-safe home as possible. Owing to the ever-changing risks, and the way in which those who would abuse technology work, it is never possible to say that any environment is 100% safe. However, we can go a long way to making it as safe as possible.

It's NOT a technical issue.

There is no magic bullet, device or program that can be installed that will guarantee your safety online. E-safeguarding is behavioural. There are, however, a few, basic technical essentials.

1) A good quality, regularly updated anti-virus, anti-spyware, anti-malware, and firewall package. Many internet service providers offer these either free, or at a substantial discount these days. They need to be installed on all your computers. Tablets and Mac computers have their own needs. Ask your supplier.

2) Every computer user in your home needs their own account. Its easy to set up and in this series, there are booklets that describe how to do this for PCs and Macs. As part of the setup, you can limit when the logon works, and by so doing, you can make sure your child isn't surfing the internet well into the night.

3) Enabling parental controls, both on computers and mobile phones is another way you can help to keep your children safe, however, remember that they may well be using computers that are not protected in this way.

Where to begin?

The first stage is an **E-Safeguarding audit** Take a look through your home, top to bottom, every drawer, cupboard, box- asking the question "What connected technology do we have in the home?"

Connected technology is anything that connects outside the walls of your home, so this includes:-

- SMART TVs
- Mobile phones
- Games consoles
- Satellite/cable TV
- MP3 players (Ipods – ipads, etc)
- Mobile hard drives

- Memory sticks

Wireless networks (Especially if they have been built by people in your family)

You may well find that you have equipment that is no longer used – old mobile phones, for example, even old computers – now is a good time to recycle them, but make sure you do so with a reputable recycling agency. Your local authority can help here.

The next step is to draw a simple map of where the items are located in your home.

Next up is what people use the technology for, so make a list of this, including things like

- Online shopping
- Social media accounts
- Online games – what games – are they played purely in the house or with users online

You may well find that each user in your home has multiple online accounts, and it is here that you will begin to understand just how varied the uses are in your home.

The next step is to sit down with your family and have an e-safety discussion. Find out what individuals know, but more importantly, what their attitude to e-safeguarding is. Do your youngsters think its all hype, or do they take it seriously?

This should lead you to a **Home Acceptable Use Policy.** In other words, an agreement for what is ok and what is not ok to do online.

Ideally, young people should write this themselves – a simple set of rules of what is ok and what isn't.

This should be done for computers, mobile phones and games consoles.

It may include things like:-

- Don't give personal information to strangers – no matter how nice they are or how well you think you know them.
- Don't use bad language or get involved in bullying.
- Don't post any image online that you wouldn't (enter name of strictest relative!)
- Don't buy anything without asking us first.

With that done, we need to think about what to do if something goes wrong.

Children are inquisitive, and they will try to go places where you would not like them to go. We all did when we were younger – why would children today be any different?

So, you need a way of them telling you they have messed up. Face-to-face sometimes doesn't work. Don't worry if your child emails you or texts you – respect the fact that they have told you, and communicate with them in the way they have chosen.

Sanctions are important.

If they break the rules, there needs to be a consequence, and the consequence must have an impact. Breaking an Acceptable Use Agreement in the workplace can have serious results – all you are doing here is underscoring that fact of life.

Sanctions need to be meaningful, so:-

- It is perfectly OK to confiscate your child's mobile phone, games station, favourite game, or even remove their access to computers in your home for a while, (they can always use school facilities for homework) if they have broken the rules.
- If they have messed up, but told you immediately, then they still need a sanction, but that sanction can be reduced. Instead of removing a cherished item for a week, do it for a day. Let them know that telling you up front has benefits.
- No child "needs" a mobile phone. If they are ill at school, the school will phone you. If you are going to be late collecting them, you can phone the school.

Keep up to date.

The e-safeguarding field changes so rapidly that it is quite understandable that parents/carers can feel swamped.

Schools can hold regular e-safeguarding events for parents/carers, and should be encouraged to do so.

The important thing is that you are not doing this alone. Other parents and carers are in exactly the same position, and you should network with them as much as possible. There is strength in numbers.

Your school will…

- Be teaching and assessing e-safety.
- Have a scheme of work that addresses the main areas of e-safety.

But what is the reality regarding e-safety in your school and in your area? Sometimes it is very easy for children to give the right answers when tested, but then go home and do the exact opposite. It is the reality of e-safety that should concern us – not getting 10/10 on the test.

This in turn means asking some serious questions.

- When did your school last have an e-safety day?
- What e-safety incidents have you had in school in the last term/academic year?

You can even ask for specific information. Don't be afraid to ask:-

- How does social networking *really* work?
- How can I use it safely?
- What are the danger signs I should look for?
- How would I know my child is being groomed?
- What if my child has already taken a "selfie" that was unwise?

If your school cannot provide this training, they have access to a support service that can.

Left Intentionally Blank For Your Notes.