Placing a device: risk assessment

The delivery model used by Connecting Scotland is based on the applicant organisation having a pre-existing relationship with the person receiving the device. This is partly because this is the most effective way to help build digital skills and confidence, but it's also about being able to manage risk better. Where there are established relationships the organisation has knowledge of the wider context of that person's life.

Being online has endless benefits, and can not only enhance a person's life, but also act as an essential lifeline. The online world can also be a harmful place, with risks of scams, harassment, bullying, harmful content, sexual exploitation and easy access to gambling platforms, to name a few. Some groups of people can be more susceptible to these online harms.

As a Connecting Scotland organisation we ask that you complete your own risk assessment when deciding who you give devices to. This may form part of your own organisational risk assessment processes (if applicable). We have provided a template that you can use to help inform your decision-making on allocating devices. This should be conducted in parallel with your own safeguarding policies, which should cover online harms.

Risk Assessment Questions:

1. Which offline risk factors may be associated with increased online risk for this individual?
2. How digitally resilient is this individual?
3. What protective vs risk factors are there in relation to the people and environment surrounding this individual?
4. What support does this individual need to achieve the greatest benefits to them of being online, whilst reducing risk?
5. Do I have all the information I need to do this assessment? How should I engage with partner organisations?

The Digital Passport is an excellent resource which could be used to inform the assessment and encourage communication about online safety between parent and child.

Risk is dynamic and can change over time. Digital Champions should be aware of any change in circumstances that can either escalate or reduce risk. We recommend that risk assessment is a continuous process.

Safeguards

A risk assessment could help identify if additional safeguards may be required. These safeguards should be informed by the outcome of your risk assessment, and could include (but are not limited to):

- Individually tailoring advice and guidance, such as in relation to a specific online risk;
- Offering additional technical safeguard support, e.g. help setting up certain parental controls;
- Devoting additional time or resources to supporting a particular individual or family;
- Sharing information with partners including local authority, school, community planning partnership etc, to understand potential risks and agree external partnership safeguarding inputs if required.

You can find more resources to help empower families, children and young people online on the Connecting Scotland website.

Some safeguarding measures that you can implement to protect children and young people online:

- Using the Google Chromebook parental controls or the iPad parental controls
- Turning on YouTube 'Restricted Mode' to help screen out inappropriate content
- Checking age ratings for any apps your child is using and check safety and privacy settings. For helpful checklists on different Apps see UK Safer Internet Centre's Social Media Checklists.
- Turning off 'location services' so your child doesn't unintentionally share their location
- Checking that App and In App purchasing require a password so things can not be bought without your permission

It is important that individuals are able to talk to someone they trust about things that they find distressing or upsetting online. This requires good communication and critical thinking skills. Harmful content can be reported to Report Harmful Content, which includes threats, bullying, violent content, unwanted sexual advances and self-harm or suicide content.