

Safer Culture North East

SAFEGUARDING FOR ONLINE SERVICES

Who is this factsheet for?

This factsheet is for employees or volunteers of organisations who are new to delivering services online/virtually and are doing so on an interim basis during the UK lockdown. It is not aimed at organisations who already deliver services online or who are beginning to do so as a result of planned delivery. The information here focuses on keeping people safe, not cybersecurity or scams, and is a brief overview of the subject. Links to more information is available at the end of this document.

Key Messages

- Safeguarding means keeping people – children and adults – safe from abuse.
- Anyone can be at risk of abuse.
- We all have a duty of care to keep people safe from harm.
- Types of abuse and harm include physical, sexual, emotional, psychological, neglect, radicalisation, discriminatory, financial.

Developing online services

Choosing and using digital platforms

These are some questions you might want to ask yourself when you're deciding which platform to use:

- Start with user needs – spend time understanding what your service users need to do, and which channels they find easy to use.
- What security features does that platform have? Can you use passwords or pin numbers to ensure privacy? Can you prevent someone unknown from joining the online space?
- Who will own the content that is posted online?
- What personal information is stored and who has access to it?
- Can the platform read personal messages?
- Think about issues around social and financial inclusion. How can you support people to access digital services?

Boundaries

- You should have a staff code of conduct that sets out clear boundaries working online and for communicating with people remotely that considers hours of work, staff ratio for working online with people, one to one working, the technology being used, etc.
- Be clear what your working hours are and when you can be contacted. Make this information part of the initial communications to manage expectations. Make sure you stick to it.

- Do not use personal profiles on social media for working or give out personal information to people you are working with. If this can't be avoided think about how you can manage this, can you set up a new social media profile specifically for this purpose for example?
- When using face to face technologies consider your home environment and what is visible on screen to others. Use a background image if necessary and possible.
- If staff or volunteers are using personal devices to deliver services, consider how to manage data protection and retention.

Keeping people safe

- Think about what your response needs to be if you see, hear or are told about someone being abused.
- Make sure all staff and volunteers know they have a responsibility to act and that they know who to speak to if they're concerned.
- Make sure you have systems in places for recording incidents and concerns, someone responsible for handling any concerns, and a safeguarding policy.
- Make sure you know how to contact your local authority safeguarding team and how to report a safeguarding concern.

Where to get more information

Risk Assessment Template for working online with children londonyouth.org/five-practical-points-as-you-rapidly-adapt-your-activities-to-the-online-world/

NSPCC online safety for organisations working with children and young people learning.nspcc.org.uk/safeguarding-child-protection/online-safety-for-organisations-and-groups/

Links to all North East local authority safeguarding partnerships and boards www.vonne.org.uk/safer-culture-north-east-resources-and-training

Links to NCVO safeguarding resources and DCMS tool knowhow.ncvo.org.uk/safeguarding/

Safeguarding awareness for volunteers video www.youtube.com/watch?v=HHQG8CJROhU&feature=youtu.be

NCPC What is Child Abuse? learning.nspcc.org.uk/media/1188/definitions-signs-child-abuse.pdf