|  |  |
| --- | --- |
|  | A picture containing drawing  Description automatically generatedA picture containing drawing, clock  Description automatically generated    In 2020, [Comic Relief](http://comicrelief.com) commissioned AVA (Against Violence and Abuse) to develop and deliver digital safeguarding training to organisations who were funded under the [Tech for Good and Tech Vs Abuse funding streams](https://www.comicrelief.com/your-impact/how-we-make-grants/tech-for-good/). This training was also offered to other organisations who were having to begin to offer online support as a result of Covid-19.  Organisations were able to attend a 90 min workshop to look at the overarching principles of digital safeguarding and some were able to attend a follow up tailored workshop to look in more detail at their chosen digital product and potential associated risks or challenges.  This resource pack was developed by AVA to accompany these sessions but can also be used as a standalone resource.  In Spring 2021 this resource pack was updated, as the pandemic continued digital safeguarding became more important and part of services longer term designs for their ways of supporting client groups. AVA has provided digital safeguarding sessions various organisations and for [The Dot Project’s](https://www.dotproject.coop/) training arm [Beyond](https://www.joinbeyond.org/) including sector discussions on specific topics like mental health, sexual/domestic violence etc.  The resources in this pack have been selected in response to requests for further information on specific topics from organisations who attended the workshops, as well as more general information that everyone should be aware of when working online.  The sections are: |
|  |  |

**About AVA**

AVA is a national charity working to end all forms of violence against women and girls. We particularly specialise in work on children and young people, multiple disadvantage and trauma informed practice. We do this via a range of research, evaluation, training, consultancy and policy work and ensure that survivors are at the heart of everything we do.

For more information about our work please visit our website: <https://avaproject.org.uk/about/>

For more details about our training (including classroom, e-learning, online interactive sessions and webinars : <https://avaproject.org.uk/training/>

You can contact us via email [info@avaproject.org.uk](mailto:info@avaproject.org.uk) and you can sign up to our newsletter for information about all our projects and training, including free sessions here: <https://avaproject.org.uk/newsletter-sign-up/>

1. **An Overview of Digital Safeguarding Principles**

A helpful place to start is with a theory about the four pillars to ensuring service user well-being online, these are put forward by the blogsite Technology Safety - who are a branch of the National Network to End Domestic Violence’s Safety Net Project:*[[1]](#footnote-0)*

**Safety** - Much of our lives are conducted online and with this comes risks for us all, these risks will be heightened if you are in an abusive situation or if you are a vulnerable adult or child. It should not be a choice between staying safe or using a platform. Strong privacy and security policies and settings, along with access to technology, help keep all of us safe. This also relates to the organisation ensuring they are properly safeguarding service users.

**Privacy** - Sharing information online should be a choice which should be open to everyone - some people will need to ensure more privacy than others if they have previous experiences with people they now need to avoid. Strong privacy policies, settings, and protections mean that service users can have control over their digital lives.

**Security:** Having a secure way to communicate with trusted individuals, seek online resources or help, or have a place to store legal, health, or other personal documents is incredibly important. Often we share our information when using online spaces, services, and apps and hope that it remains secure. Strong security measures help ensure that personal information does not get into the wrong hands.

**Access:** Building a platform that is intentional in centering the needs of service users means considering the accessibility needs of those who live with disabilities, speak another language, or have culturally-specific privacy and safety needs. Accessibility barriers that keep victims from getting assistance can be a significant safety risk. Making sure that we have accessible products, platforms, and technologies should be a core tenet of your work.

**Digital safeguarding**

Digital safeguarding is much like safeguarding in any other context. Safeguarding, under The Care Act (2014), means protecting children and vulnerable adult’s right to live in safety, free from abuse and neglect. It is about people and organisations working together to prevent and stop both the risks and experience of abuse or neglect.

A safeguarding risk involves an allegation or concern that a person has or may have behaved in a way that has harmed themselves or another person, or behaved towards a child(ren) or adult(s) in a way that indicates they may pose a risk of harm to others. Safeguarding is an organic process, individuals holding the risk must look at each context in its own light and must recognise that adults and children sometimes have complex interpersonal relationships and may be ambivalent, unclear or unrealistic about their personal circumstances.

As with all safeguarding, online safeguarding involves a whole rubric of potential harms; and must be looked at in relation to both victim and perpetrator.

As with all safeguarding and handling of potential risk, organisations and individuals must adopt a strong moral framework through which to design, implement and ensure the safety and wellbeing of all those they are supporting. Where issues arise without clear ‘do’s’ and ‘don’ts’ or where best practice has not otherwise been established, work within this moral framework, share learning with others and crucially, speak to those you hope to support and ask for their advice and input regularly.

[Here](https://knowhow.ncvo.org.uk/safeguarding/what-is-safeguarding) is The National Council for Voluntary Organisations’ guide to what safeguarding is.

[Here](https://learning.nspcc.org.uk/safeguarding-child-protection#:~:text=Safeguarding%20is%20the%20action%20that,children%20from%20abuse%20and%20maltreatment&text=ensuring%20children%20grow%20up%20with%20the%20provision%20of%20safe%20and%20effective%20care) is the NSPCC’s comprehensive definition and resources around safeguarding children and child protection.

Care Check is a leading umbrella body for the (DBS) Disclosure and Barring Service, read [their guidance](https://www.carecheck.co.uk/importance-of-safeguarding/) on why safeguarding is so important.

**The 6 principles of safeguarding:**

The Care Act (2014) outlines the responsibilities of individuals to safeguard vulnerable adults and children in a manner which encourages a holistic person-centred approach.

Taking a person-centered approach to safeguarding means placing the individual’s wellbeing at the forefront of any concern and involving them (as much as possible) in any safeguarding procedure.

The Care Act (2014) sets out six core principles to enable this:

|  |
| --- |
| **Empowerment**  *encouraging individuals to make their own decisions, ensuring consent, putting people first, keeping individuals informed*  **Protection**  *responding quickly and effectively to protect individuals from harm, supporting individuals to take action*  **Prevention**  *ensuring a proactive approach to safeguarding and risk management*  **Proportionality**  *accounting for each situation in its own right when making decisions relating to protection and support*  **Partnership**  *partnering with local organisations and agencies to prevent and protect as proactively as possible, sharing useful and appropriate information where necessary*  **Accountability**  *maintaining transparency in all safeguarding practices, making sure roles are clear and defined* |

By keeping these principles in mind during any safeguarding procedure, an individual's safety can be ensured without removing their autonomy.

**Organisational responsibility and digital safeguarding**

[Girl Effect (2018)](https://prd-girleffect-corp.s3.amazonaws.com/documents/Digital_Safeguarding_-_FINAL.pdf?AWSAccessKeyId=AKIAIWVYO5R6RMTXA2NA&Signature=OTVVCMSYMTYuSEOXD0blrvPCpds%3D&Expires=1612958408)[[2]](#footnote-1)[, have published an in-depth guide](https://prd-girleffect-corp.s3.amazonaws.com/documents/Digital_Safeguarding_-_FINAL.pdf?AWSAccessKeyId=AKIAIWVYO5R6RMTXA2NA&Signature=OTVVCMSYMTYuSEOXD0blrvPCpds%3D&Expires=1612958408) detailing the intricacies of online safeguarding. Below is a diagram they have created representing the areas in which digital safeguarding takes place:



|  |
| --- |
| Ensuring the privacy of individuals in the digital realm includes thinking about: **consent, anonymisation, data collection and storage, GDPR and Data Privacy Impact Assessment (DPIA)**.   * DPIA: A Data Protection Impact Assessment is a process to help you identify and minimise the data protection risks of a project. You must do a DPIA for processing that is likely to result in a high risk to individuals. Information on performing a DPIA is available from the Information Commissioner's Office (ICO) [here.](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/) * Looking at a project through the ‘privacy lens’ at an early stage can act as a ‘warning light’, highlighting potential privacy risks before they materialise and whilst measures can be put in place to reduce the risks. |

|  |
| --- |
| Ensuring the security of individuals in the digital realm includes thinking about: **the tools and IT you use, passwords, encryption, GDPR.**   * The Information Commissioner's Office (ICO) website offers in-depth guidance for overall organisational security measures, [here.](https://ico.org.uk/for-organisations/guide-to-data-protection/) |

Organisations should have **clear policies and processes around safeguarding, data protection and liability**, particularly when children and (vulnerable) adults are sharing personal information.

You can choose to integrate safeguarding policy for offline and online activities or create a specific digital safeguarding policy.

[Here](https://bswaid.org/policies-and-procedures/safeguarding-children-young-people-policy-procedures/) is a publicly available example of safeguarding policy and procedures by Birmingham and Solihull Women’s Aid.

[Here](https://knowhow.ncvo.org.uk/safeguarding/steps-to-a-safer-organisation/safeguarding-day-to-day) is The National Council for Voluntary Organisations’ on how to review your policies regularly and ensure everyone with safeguarding responsibilities feels supported.

|  |
| --- |
| A digital safeguarding policy should determine:   * definitions of behaviours, such as online abuse and harassment, image-based abuse, identity fraud and exploitation (detailed later in this resource pack). * expected standards of conduct across staff and users, including standards related to privacy and security * sanctions for those who breach these standards * a standard safeguarding procedure and designated safeguarding lead |

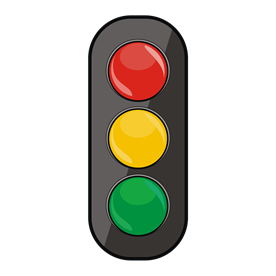
Embedding safeguarding requires identifying and assessing potential risks to individuals (how likely and how severe); and identifying any additional measures to mitigate those risks. When working to embed safeguarding in online spaces, it is important to consider the 6 safeguarding principles and how these can be adapted to the digital environment.

**Empowerment** demands listening to the voices of those one intends to protect and support.  Including those with lived experience or potential service-users is fundamental to understanding and working towards managing potential risk[[3]](#footnote-2). Thinking about **protection** online demands thinking about what steps can be taken to make sure people are safe to use the resources/tools being developed, whilst **prevention** might include doing assessments to understand potential risks prior to launching platforms.

Maintaining a **proportional** response is still key, and this includes recognising the serious nature of risk online and creating clear and proportional policies to prevent and protect individuals from this. Creating **partnerships** should involve teams thinking about services and organisations currently being run online, learning from their skill base and staying in contact with other organisations and relevant authorities.

**Accountability** is just as important when working online and through adopting and embedding the considerations detailed in this resource, organisations can ensure they are maintaining accountable and transparent working practices.

*Procedures for managing, preventing and working through risk are detailed in the remainder of this resource pack.*

**2. Risk Assessment Online**

For those working with people who are more vulnerable to online risks, it can be hard to know where to start. A good starting point is to identify the nature and scale of the risk. As with all safeguarding, consider the person’s wants and needs, abilities, experiences and influences (where possible).

### **Risks are likely to fall into three main categories:**

* Delivery practice: protecting people when using online technology to engage them. Think video calls, messaging apps, interactive chat spaces etc.
* Privacy and consent: respecting and ensuring people’s privacy and choice when engaging them digitally. Because activity and details can be more visible online
* Information security: protecting your systems and people’s data from misuse and unauthorised access. Technical security is important but staff behaviour makes the biggest difference.[[4]](#footnote-3)

**Digital risk**

When broken down into its component areas of risk, safeguarding is fundamentally concerned with behaviours. There are a considerable number of avenues through which safeguarding concerns might arise in digital spaces. These can be split into three key categories;

|  |
| --- |
| * **Content** – this is content that may be unsuitable or illegal. This might include pirated content or offensive language and behaviour. * **Contact** – this may be unwanted or inappropriate contact, such as grooming or unsolicited sexual contact * **Conduct** – this could be as a recipient or as an active participant – oversharing personal information or the bullying of another person |

Within these three categories, there are multiple avenues in which individuals might incur harm. These include, but are not limited to:

* Exposure to inappropriate or harmful material online e.g. gambling content, pornography or violent content
* ‘Digital’ self-harm[[5]](#footnote-4)
* Problematic internet use (internet “addiction”)
* Exposure to content that promotes worrying or harmful behaviour e.g. suicide, self-harm and eating disorders
* Becoming victims of cybercrime such as hacking, scams/hoaxes, fraud and identity theft
* Radicalisation and extremism online
* Online abuse.

*Online abuse and potential risks online are explored in depth in section 3 of  this resource.*

At all stages, risks need to be considered both in relation to user and provider. Considerations need to be made in relation to necessary safeguards to be put in place so that everyone can be confident about the service. What safety measures, systems and processes are required to make this happen?

**Creating a risk assessment matrix**

A risk assessment matrix or register is a useful tool to assist teams in ensuring risks are considered in-depth and reduction measures embedded in online safeguarding policies and procedures. Risk assessment matrices need to be developed in relation to the tool being used/created and will therefore differ. A basic template risk assessment matrix is illustrated below and should be used when developing any new digital service or product. It should also be regularly reviewed and updated.

|  |  |
| --- | --- |
| **Risk** | **Considerations** |
| **Potential risk** |  |
| **Likelihood of risk** |  |
| **Severity of risk** |  |
| **Reduction measures to implement** |  |

Risks should be considered in relation to the three key areas of digital risk:

|  |
| --- |
| **Content** risks involve inaccurate, harmful and illegal content.   * *Ensure clear rules for users that address the issue of what constitutes inappropriate content in the context of a specific online well-being service. This includes what staff post as you may be liable for inappropriate content.* |
| **Contact** risks involve inappropriate and unwanted contact between users. This includes any contact in which one user may exploit another.   * *Always vet staff who have access to the site (DBS)* * *Be vigilant to inappropriate content between users – make sure there is something in place for them to report anything they are concerned about.* * *Make sure to use reporting structures with police, child exploitation online protection centre (CEOP) etc.* |
| **Conduct** risks relate to how people behave online. Can include bullying, trolling, abusive comments.   * *Establish clear guidelines, escalation policies and reporting mechanisms as above.* |

Youth Links Scotland have also created a resource for assessing the risk of *not* using digital technology when working with young people (in particular), available [here.](https://www.youthlinkscotland.org/media/3546/risk-assessment-not-implementing-digital-youth-work.pdf)

**Creating a new digital product**

When **creating a new digital product,** you may not need to do a DIPA, but you should always incorporate a risk assessment when using or creating digital tools for working with vulnerable individuals. Risk will inevitably relate to the nature of the product at hand, but below are some key considerations for any risk assessment taking place online;

|  |
| --- |
| * Describe the nature, scope, context and purposes of the data you will be collecting/processing * What will you do with it? Who will you share it with? How will you store it? * How safe is the online product for the user? * Are they able to access it in a confidential space? * How to reduce risk of a potential perpetrator finding out? * How can you assess risk online – what will be different to face to face? * How can you carry out appropriate safety planning? |

**Typical safeguarding/escalation pathway**

It is impossible to consider every potential risk that might arise in an online space or through the use of a digital tool. As with working with or supporting individuals face-to-face, relations are organic and risks will emerge that might not have been foreseen. Those concerned about an apparent risk will need to respond quickly and effectively to mitigate any potential harm as far as possible.

Creating a pathway to manage emergent risks is crucial to ensuring a streamlined response. Below is a typical example of a safeguarding pathway:

|  |
| --- |
| As with all safeguarding, all teams/organisations should have a named person who manages safeguarding concerns. This may be the **designated lead for safeguarding**, or another individual tasked with managing risk in your organisation’s online operations.   * Designate a digital safeguarding lead * Ensure all relevant teams/staff are made aware of the designated safeguarding lead |
| Anyone who becomes aware of an online safeguarding incident should **record the facts** and information as for any other Protection concern.   * This should be passed on to the safeguarding lead promptly * Ensure all correct and relevant information is passed on * Pass on information as quickly as possible |

|  |
| --- |
| The designated safeguarding lead or team will decide whether the person is at immediate risk of harm. If they are, the authority will **take action.** This could mean removing the person from the harmful situation, or removing the person causing the harm.   * Where a person is deemed to be at risk of significant harm, they must be encouraged to call emergency services (999) or offer to do so on their behalf. * *If an individual is anonymous to you (e.g. using a pseudonym), validate what they are going through, explain that you are very concerned for their safety, recommend that they call emergency services or offer to do it on their behalf.* *You may not be able to support them in seeking help, if this is the case, look after your own wellbeing and debrief with trusted colleagues.* * *Your organisation will have to make a collective decision as to whether you are willing (and able) to access the IP addresses of individuals using your platform. If this is the case, this should be made clear to all users in case there are instances in which you break confidentiality to ensure their safety.* * In accordance with the principle of ‘proportionality’, there are many different courses of action. * The safeguarding person or team will decide whether they need to investigate the issues any further |

|  |
| --- |
| In order to ensure transparency and accountability, all evidence must be collected relevant to the apparent risk.   * Take all necessary steps to stop the device from being used – if it is safe and possible so to do * Do not delete any evidence e.g. images, messages. If able, ensure the device is placed in a secure place so evidence cannot be destroyed or the individual further abused. * Do not copy any evidence, screenshot or print where possible. * Write down what has been seen or sent * In the case of evidence involving an illegal image, for example, pornograpy involving illegal acts or indecent images of children, seek advice from [CEOP](https://www.ceop.police.uk/safety-centre/) or the police around how best to handle such evidence.   *More information related to ethical evidence collection, see* [*Girl Effect*](https://www.girleffect.org/stories/digital-safeguarding/) *(2018)* |

|  |
| --- |
| As mentioned above, the response to a safeguarding concern is likely to vary greatly. The safeguarding lead and relevant team members will consider the individual’s situation and context as much as possible and react accordingly. Further inquiry and protection measures might involve:   * Discussing the issues with the adult/child themselves * Discussing the issues with other professionals responsible for the adult/child’s care * Building up a more detailed picture of the situation at hand through partnership working and further investigation * Considering prevention measures that can be put in place to prevent the vulnerable adult or child from being abused and neglected |

Most importantly, cases where risk does emerge and needs to be managed must be taken as **learning** opportunities which can be used to improve preventative measures and safeguarding procedures in the future.

[Here](https://www.thecatalyst.org.uk/blog/how-to-risk-assess-your-preferred-third-party-platform-for-online-service-delivery) is an article from Catalyst on “How to risk assess your preferred third party platform for online service delivery”.

**3. How Technology Can be Used to Abuse and Control**

In today’s world, technology is unavoidable and constantly changing. Although many forms of technology offer services and survivors’ opportunities for support and safeguarding, they also offer perpetrators a new toolbox of ways to stalk, exploit, isolate and control women and children.

A recent survey Comic Relief[[6]](#footnote-5) found that 47% women who had experienced abuse had also had their online activity monitored by their partner and 25% said they did not know if this was happening or not (highlighting the covert nature of some of the ways victims can be monitored and controlled online). The report found that: ‘*Online harassment is intersectional, often incorporating sexism, racism, homophobia, and other forms of oppression. Abusers may use a vast array of online tactics to harass their victims*’.

AVA recently surveyed 82 victims of domestic abuse and 54% confirmed technology had been used as part of the abuse.

**Useful definitions:**

**Coercive control** - an act or a pattern of acts of assault, threats, humiliation and intimidation or other abuse that is used to harm, punish, or frighten their victim.

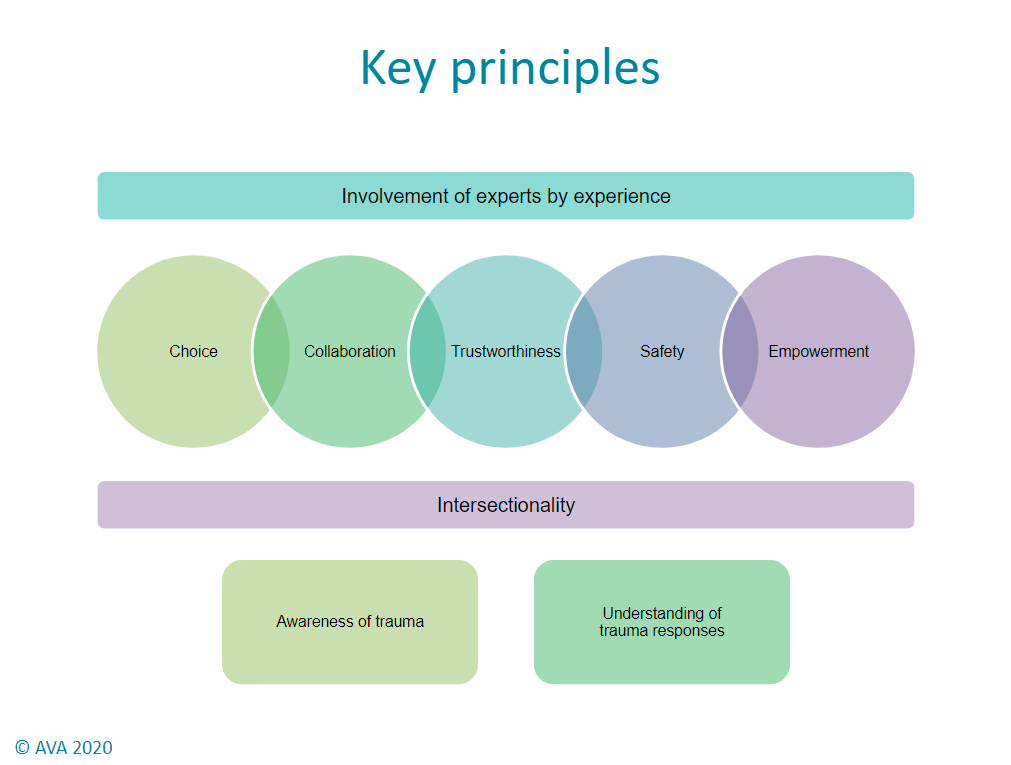
This controlling behaviour is designed to make a person dependent by isolating them from support, exploiting them, depriving them of independence and regulating their everyday behaviour.[[7]](#footnote-6)

**Trauma -**  The Diagnostic and Statistical Manual (5th edition), which is used to diagnose post-traumatic stress disorder, describes traumatic events as: “exposure to actual or threatened death, serious injury or sexual violation. The exposure must result from one or more of the following scenarios, in which the individual:

* directly experiences the traumatic event;
* witnesses the traumatic event in person;
* learns that the traumatic event occurred to a close family member or close friend (with the actual or threatened death being either violent or accidental); or
* experiences first-hand repeated or extreme exposure to aversive details of the traumatic event (not through media, pictures, television or movies unless work-related).”

**Trauma Informed Services -** [Harris and Fallot’s work](https://pubmed.ncbi.nlm.nih.gov/11291259/) identified five core domains that services need to address to become trauma informed. Some of these are similar to the six safeguarding principles:

* *Choice* – services users are supported in taking control of their lives. The first step is enabling service users to choose how they access the support that is offered.
* *Collaboration* – service provision is a partnership between staff and service users. This is a stepping stone to developing trust as well as the foundation for empowerment.
* *Trustworthiness* – trustworthiness is in the middle of our model as building trusting relationship with service users is key to being trauma informed.
* *Safety* – services should feel physically and emotionally safe to service users
* *Empowerment* – service users’ self-efficacy is promoted.



**Examples of How Technology Can Be Used to Abuse**

There are a range of tactics that may be used by abusers online, the list below is not exhaustive, but covers some of the most common:

* Demanding passwords
* Constant checking of phone/social media
* Threats via messaging, email, social media
* Identity theft
* Malicious comments to discredit
* Removal of all tech to isolate
* Using apps to gain access to a webcam
* Threats to share images/‘Revenge porn’
* The use of ‘spyware’ to monitor someone online
* Setting up alias accounts
* Repeated and constant messaging
* Hidden cameras
* Recording devices in children’s toys
* Using GPS technology to locate
* Using Geo-tagging technology in photos

The Internet of Things (IoT) is an umbrella term that describes interconnected ‘things’ and systems which are the direct extension of the internet into a range of physical objects and devices.Basically, this includes products which have become digitally ‘smart’ such as Amazon Echo, Google Home, Philips Hue, Fitbits etc. Again, these devices offer perpetrators additional ways to monitor, control and abuse victims. For more information, see the [guide from UCL here.](https://www.ucl.ac.uk/research/domains/sites/research_domains/files/gender-iot-tech-abuse.pdf)

[Here](https://www.techsafety.org/iot-overview) is a guide by Technology Safety about types of devices and ways to enhance the safety and privacy of them.

Stalking is generally understood as a pattern of repeated and unwanted attentions, communications and contacts in a way that causes distress, fear or alarm.

*Online stalking/harassment:*

* 23% of women polled in an Amnesty International study across the eight countries said they had experienced online abuse or harassment, 22% in the UK[[8]](#footnote-7).
* 78% of those who’ve dealt with cyber stalking/stalking with a cyber element had a PTSD diagnosis [(Suzy Lamplugh Trust).](https://www.suzylamplugh.org/)

Cyber-stalking is a less researched and newer form of stalking that appears in many reports of IPV. Cyber-stalking and abuse can involve various forms of technology, and often involves threats related to reputation, physical injury, impersonation[[9]](#footnote-8)[[10]](#footnote-9).

It is crucial to consider how your chosen digital product may be misused by perpetrators, or how they may be tracking the devices, apps and programmes used by victims and children. Even after separation from an abusive relationship, tracing devices, spyware and cameras may still remain on devices and in homes, therefore you must assess the safety of your platforms and of the devices used by those using your products. Always ask about previous experiences of tech abuse when assessing new users. And remember, that if someone has experienced tech abuse, they may be more fearful or mistrustful of accessing support via tech and may need some additional reassurance and support.

**Below are some tips to bear in mind when advising victims and when developing safety plans:**

* Review what information exists about the victim online (this can also be useful for practitioners to do for themselves)
* Ensure all devices have updated antispyware software installed and turned on
* Keep all privacy settings on social media accounts up to date
* Turn off all GPS and location sharing settings
* Regularly change email and passwords
* Avoid sharing photos that may identify your location or any personal information
* Request to be notified before anyone can check you in or tag you on facebook
* Make sure wireless hubs and routers have security options turned on
* All risk assessments to routinely ask about experiences of digital abuse
* Collect and save any evidence from social media sites (prior to asking for it to be removed)
* Keep recordings of calls and voicemails
* Document and report incidents.

**4. Platforms and Facilities**

Using digital platforms and facilities is an increasingly common and useful means of staying in contact with and supporting vulnerable adults and children. These tools not only allow for new forms of contact, but for contact to be consistent when individuals might not be able to access appointments or feel unsafe to do so.

These online platforms provide a variety of plus points, but can also incur different risks. These risks are related to both the functioning of the platform itself, e.g. its security and privacy procedures, and the way in which the platform is used, for example, if the individual uses it in a safe space or safe way.

**Using/creating digital platforms to support vulnerable clients**

**The first step** when using digital platforms to support vulnerable clients is ensuring usability. Assess the client’s digital literacy and accommodate for their circumstances (i.e. do they only have access to a smartphone rather than a laptop, do they feel comfortable video chatting?). Keep the client involved in any decision to switch to or use digital means of communication, offering choice and information related to potential platforms.

*If creating a new digital platform:* consider the needs and capabilities of the client group. Involve your intended user group in formulations.

|  |
| --- |
| *For example, when considering what tools to use with a victim/survivor of domestic abuse where a face-to-face appointment is not possible, a support worker might consider; the service user’s digital literacy, language, access to technology, potential trauma response to different technologies (for example, a victim/survivor might prefer to video chat as it provides an extra level of security in knowing who they might be talking to)* |

It is necessary to think about the digital skills of the client group when designing digital services. The UK Government have created an Essential Digital Skills Framework - this reflects the range of skills people need to safely benefit from, participate in and contribute to the digital world.[[11]](#footnote-10)

They outline five key skill groups:

**Communicating** - communicate, collaborate and share online

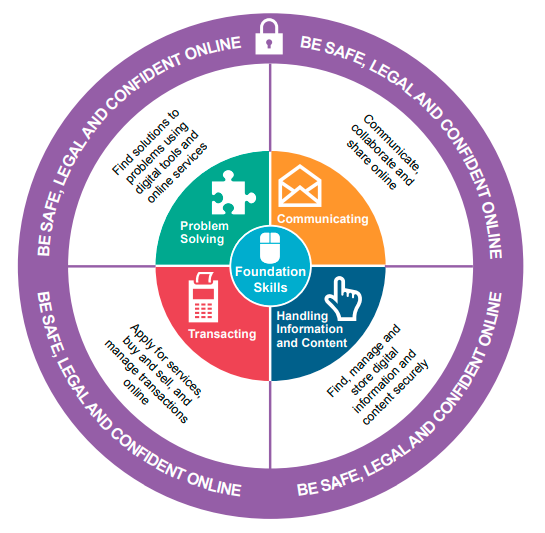
**Handling information** - finding, managing and storing digital information and content securely

**Transacting** - apply for services, buy and sell, manage transactions online

**Problem solving** - find solutions to problems by using digital tools and online services.

The fifth skill - **being safe, legal and confident online** - is embedded across the other four.

FutureDotNow have shared itemised skills with examples across the foundational skills, see [here.](https://futuredotnow.uk/the-essential-digital-skills-framework/)



**The second step** in ensuring safe and secure working practices when using digital platforms is reading up on the data and privacy protection measures they have already put into place. If using platforms or digital tools to support vulnerable individuals, the importance of staying informed is crucial to ethical working practices. If you are adapting your working practices to using digital tools, you are responsible for understanding and passing forward information related to your client’s privacy and security.

*If creating a new digital platform:* consider the need to embed privacy and security considerations (as explored in sections 1-2). Ensure simple and easily accessible safety and privacy information is available for users.

|  |
| --- |
| *For example, when using a video-chat tool to engage with a victim/survivor of domestic abuse where a face-to-face appointment is not possible, a support worker might consider; whether the chat is sufficiently encrypted, exit buttons easily accessible to the client, etc.* |

Once you have a full understanding of the privacy and security implications of using this platform, this must be translated to your service user/client effectively to ensure that they are equally informed. Be mindful that they might not be as digitally literate as you, try to use simple terminology and keep information as clear as possible.

**A quick note on important guidelines to be aware of**

* [The Data Protection Act, 20218](https://www.gov.uk/data-protection) is the UK’s implementation of the General Data Protection Regulation (GDPR)
* [GDPR](https://gdpr-info.eu/)
* The UK legal age of consent for accessing online services is 13. [Read the report Children and the GDPR.](https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/children-and-the-gdpr-1-0.pdf)
* [GDPR Article 8](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/children-and-the-uk-gdpr/what-are-the-rules-about-an-iss-and-consent/) offers more guidance around consent when working with children.
* [Online Harms White Paper](https://www.gov.uk/government/consultations/online-harms-white-paper): “The government wants the UK to be the safest place in the world to go online. The government also wants the UK to be the best place to start and grow a digital business. They are therefore creating a new regulatory framework to make sure people are safe online.”[[12]](#footnote-11) The results of this consultation will impact online services you are conducting or will create in future. [This easy read summary](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/811923/EASY_READ_Online_Harms_White_Paper.pdf) defines keys words throughout.
* We recommend you keep track of the EU’s ePrivacy rules. Children’s Commissioner’s (Dec 2020): “...new EU ePrivacy rules came into effect which introduced new limits on the way in which technology companies can use messaging and calling data. The rules undermine the ability of companies to use established, privacy-preserving tools such as PhotoDNA to identify child sexual abuse imagery and grooming on their platforms. Five companies, including Google, Microsoft and Roblox, have publicly committed to continue proactively scanning their platforms for illegal child abuse material regardless, while the EU finds a solution. I would strongly encourage all platforms to follow their lead and continue scanning for this material, until the EU has concluded its discussions on an exemption.” Read the full statement [here.](https://www.google.com/url?q=https://www.childrenscommissioner.gov.uk/2020/12/23/statement-on-new-eu-eprivacy-rules-and-the-implications-for-children/&sa=D&source=editors&ust=1612972469482000&usg=AOvVaw06-1bJtb62HuNQezUaYzo1)
* We recommend thinking about end to end encryption in messaging services used by children and keeping up to date with the p[lans by tech giants for more encrypted messaging risks greater child exploitation and abuse - December 2020](https://www.childrenscommissioner.gov.uk/2020/12/08/plans-by-tech-giants-for-more-encrypted-messaging-risks-greater-child-exploitation-and-abuse/). This report by the Children’s Commissioner [“*Access Denied: How end to end encryption threatens children’s safety online”*](https://www.google.com/url?q=https://www.childrenscommissioner.gov.uk/report/access-denied-how-end-to-end-encryption-threatens-childrens-safety-online&sa=D&source=editors&ust=1612973049281000&usg=AOvVaw0FedjkT_Xrh_ZfCOF3m0ym)looks at children’s use of private messaging services like WhatsApp and Facebook Messenger. The study suggests that millions of children in England are using messaging platforms that they are not old enough to be accessing. The report comes following announcements by Facebook, and indications by other platforms that they plan to apply end-to-end encryption to all their messaging services. End-to-end encryption makes it impossible for the platform itself to read the contents of messages, and risks preventing police and prosecutors from gathering the evidence they need to prosecute perpetrators of child sexual exploitation and abuse.

**The final step** to consider when using digital tools and online platforms is to ensure that the context in which they are being used is safe. It is important to consider the environment in which the client/service user is engaging. Are they living in shared accommodation where another individual might be able to read your conversation? Are they in a public place where having intimate conversations might be inappropriate? Are there children or young people in earshot of a conversation?

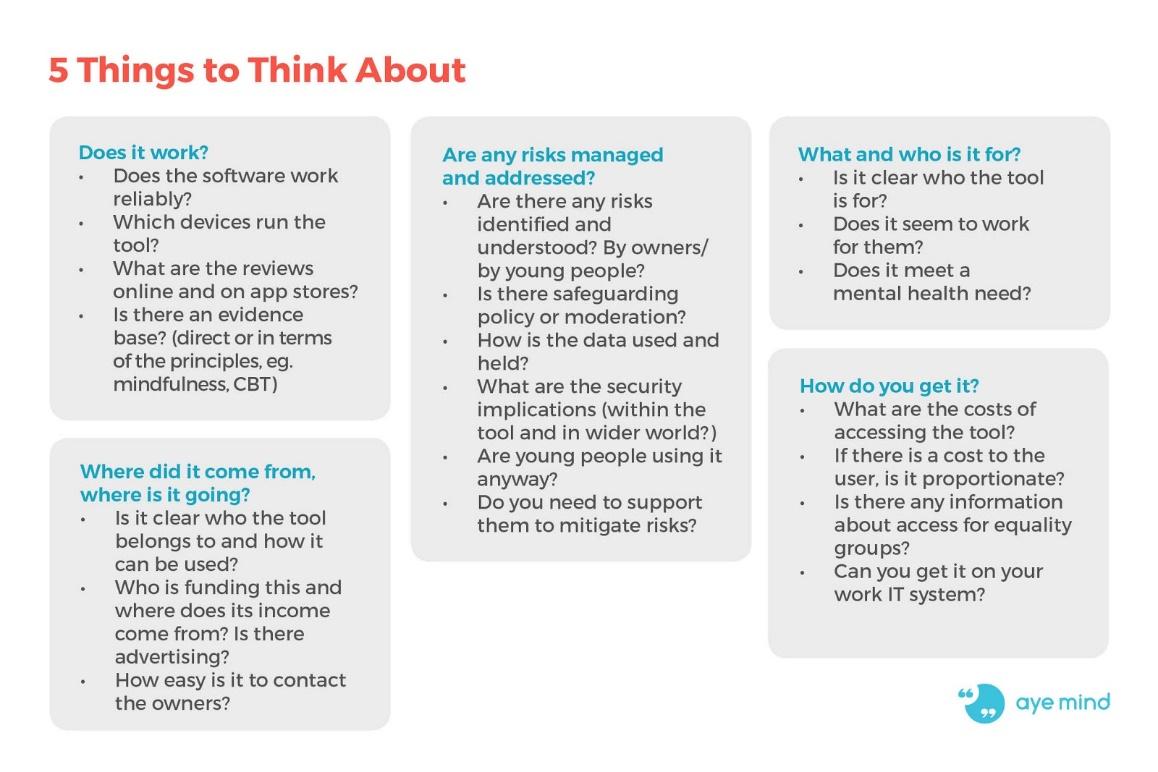
*If creating a new digital platform:* consider what medium the platform is best suited for (e.g. phone, tablet, computer) and safe contexts in which to use it. Provide tips or a user manual.

|  |
| --- |
| *For example, when using a video-chat tool to engage with a victim/survivor of domestic abuse where a face-to-face appointment is not possible, a support worker must consider; could someone overhear a conversation? Could this conversation be accessed by a perpetrator?* |

Discuss safe and secure environments in which to use online platforms with your clients, for example, encourage them to find a safe and quiet place away from others when video chatting. In the case of individuals living with abuse, you might want to establish a safe-word or code in case a perpetrator enters a room/house when video chatting in order to end conversations and alert you to risk quickly without detection.

**Key to maintaining effective communication and support is to include the individual you are supporting in making decisions about what tools work best for them. Make sure to consider each individual’s comfort levels in accordance with their specific circumstances, especially in relation to individuals who have experienced trauma or are in high risk situations. Always offer options and choices.**

Below is a chart of considerations for those hoping to use new digital platforms and tools from [Ayemind](http://ayemind.com).



**What medium works for me?**

Different digital tools will suit different individuals at different times. When discussing which forms of contact to use with clients or service users, or when formulating new digital products,

it is important to consider the potential pros and cons of using a particular medium of communication.

The Catalyst, a network supporting charities to strengthen their digital capacities, provide numerous resources to assist charities when choosing the right digital tools for them, available [here.](https://www.thecatalyst.org.uk)

*Below is a list of some of the key pros and cons, alongside some safety tips, to consider when creating or adapting communication to use with vulnerable adults or children. For each of these modes,  there are key considerations that should be made and that will need to be thought through. This can be done as part of your risk assessments.*

**Email**

Emails enable contact between two (or more) people in a delayed format. This allows for easy communication of long form information, leaving time for recipients to consider and read over any detail in their own time. This also allows users to think and reflect on the content and information they are sharing in more depth.

Despite this, there are some key considerations or downsides of email communication. Considering the contact is entirely behind the screen, one cannot be entirely sure of who is reading, accessing and replying to emails. Furthermore, the abundance of emails individuals are likely to receive daily (especially at work) means that emails are not well suited to crisis situations where opportunities for support might go unread or unnoticed for a number of hours.

|  |
| --- |
| *Safety and security considerations:*   * Think about who has access to the email account(s) * Are emails being saved? * Who is saving them and is it safe to do so? * Do you have another (faster) means of contacting the individual if a concern or risk is apparent? |

Get Safe Online have created guidance on using emails safely, available [here.](https://www.getsafeonline.org/online-safety-and-security/email/)

**Live Messaging/Instant Chat**

Live messaging and chat apps enable instant two way communication. This can be incredibly effective and helpful, especially in crisis situations or where the need for support is immediate. Encrypted chat apps provide safe communication in circumstances where it might not otherwise have been possible.  Despite this, as with emails, who is reading, accessing and responding to messages is never entirely clear.

|  |
| --- |
| *Safety and security considerations:*   * Think about who has access to the messaging app? * Are messages being saved? * Who is saving them and is it safe to do so? |

*Examples:* Women’s Aid run a live chat service, available [here.](https://chat.womensaid.org.uk)  Victims Support run a live chat service, available [here.](https://www.victimsupport.org.uk/help-and-support/get-help/support-near-you/live-chat)

**Video calling**

Using video calling apps can be a  beneficial means of staying in contact in a more intimate and personable fashion than messaging or emails might allow for. Video calling can be a great way to offer support and communicate conversationally when distanced. Despite this, not all video calling apps are as safe as each other.

|  |
| --- |
| *Safety and security considerations:*   * Can others access your video chat? * Does the individual feel safe/comfortable showing their face? |

Age UK provide a simple guide to setting up video calling on various different platforms, available [here.](https://www.ageuk.org.uk/information-advice/work-learning/technology-internet/video-calling/)

**Chatbots**

Chatbots are computer programmes which simulate conversations. These can be used for platforms where users want information, and are becoming increasingly popular. When well thought out and designed, they can be a means of offering information, in a cost-effective and scalable manner. Despite this, chat bots might provide misinformation (outdated, inappropriate, irrelevant). Inadequate responses might upset or frustrate individuals looking for answers, leaving them less likely to otherwise seek help.

|  |
| --- |
| *Safety and security considerations:*   * Is the chat bot regularly updated? * Is the user being signposted to relevant information? * Are users aware that they are not speaking to an individual? * Are responses empathetic and validating? * Has the chatbot been coded to ensure assumptions are not made? |

Using chatbots to provide advice of any sort should be done cautiously, especially considering the potential to give outdated or inappropriate advice. Be sure to make the limits and purpose of your chatbot clear so users are aware of what service is being offered.

UNICEF have produced a brief relating to the creation of chatbots for young people’s advice services. This resource is relevant for any service looking to create chatbots, and is available [here.](https://www.unicef.org/eap/media/5376/file)

Bauer et al’s (2019) paper on building a chatbot for survivors of sexual harassment is available [here.](https://arxiv.org/abs/1909.02809)

**Forums/message boards (moderated and unmoderated)**

Forums are a great way for individuals to react, share knowledge and resources relating to shared experiences. They are also a useful medium through which providers/support workers can find out information about particular issues and provide advice in a fast and effective manner.

Unmoderated forums allow for an equal input from all parties and an organic approach to building knowledge and relationships. Despite this, when creating forum boards for those who might have negative or emotive shared experiences, moderating a platform is often the best means of ensuring the safety and wellbeing of all.

|  |
| --- |
| *Safety and security considerations:*   * Is it safe for this group of users to be interacting without moderation? * How will you deal with disclosures? * How will you support individuals triggered by others disclosing? * Those creating forums should discuss and create guidance on what is going to be allowed on the board and what is not, with a clear policy on when things need to be escalated. * Ground Rules and expectations should be made clear to all users. Individuals might post traumatic experiences that may trigger others, suggestions that they are at risk of harming (themselves or others) or inappropriate personal information. * How will you ensure a safe and equal space for all? For example, will you limit topics of discussion to predefined areas? * Inappropriate behaviour should be moderated and users informed if their posts are removed or edited. *Tips for moderating platforms are presented later in this section.* |

A guide on setting up forums is available [here](https://www.webhostingsecretrevealed.net/blog/blogging-tips/starting-and-running-a-forum-for-your-website/).

**Peer Support/Live Chat forums**

Live chat forums, as with other forums, can be a brilliant means of peer support through which individuals can share their experiences and feel validated and understood by others. It is important to consider the nature of online forums, especially the fact that disclosures are often more likely to happen online, [see John Suler’s paper on ‘online disinhibition’.](http://drleannawolfe.com/Suler-TheOnlineDisinhibitionEffect-2004.pdf)

[Here](https://www.onlinetherapyinstitute.com/2009/02/25/the-online-disinhibition-effect/) is a shorter article by the Online Therapy Institute.

Moderators or those supporting the platform must be ready for disclosures and, as with moderating forums, clear and streamlined procedures must be in place for contacting the individual and escalating if needs be.

|  |
| --- |
| *Safety and security considerations:*   * Is it safe for this group of users to be interacting without moderation? * How will you deal with disclosures? * How will you support individuals triggered by others disclosing? * See the section on online forums for further considerations. *Tips for moderating platforms are presented later in section 7.* |

Mind and McPin’s guide to managing peer support groups includes tips on creating online peer support spaces, available [here.](https://www.mind.org.uk/media/17944275/peer-support-toolkit-final.pdf)

Catalyst’s article on Internet Forums - how to take a safety first approach to connecting vulnerable people online, [see here.](https://www.thecatalyst.org.uk/blog/forums-a-safety-first-approach-to-connecting-people-online)

**Gaming**

Gaming can be a creative and interactive way to use tech for communication and support. Using games can be a means of transferring information in a fun and novel way, especially with young people. As with any other digital product, one needs to make sure that it is safe and risks are foreseen and considered.

Games often allow individuals to play in an anonymous fashion, and this needs to be considered in relation to individuals potential disinhibition, or those that adopt false personas.

|  |
| --- |
| *Safety and security considerations:*   * Clear policies should be put in place in relation to conduct, especially where games enable individuals to message live. Considerations might include: policies related to language, policies related to the sharing of personal information, policies related to the sharing of contact information * If you are creating a game for young people, how are you ensuring that only young people can access it? Is the content age appropriate? |

*Tips for moderating platforms are presented in section 7.*

Jennifer Ann’s group has created Gaming Against Violence which produces and publishes video games designed to prevent teen dating violence. More information available [here.](https://jenniferann.org)

Ayemind provide resources on working with young people, as well as a database of resources including a number of games, available [here.](http://ayemind.com/resource-map/)

**Blogs**

Blogs can be a brilliant means of both sharing easy read information and giving advice in a less prescriptive fashion. For those who have lived experience of abuse or disadvantage, writing blogs can be both therapeutic and empowering. For many, blogs are a good medium through which to share their experiences. There are some considerations that need to be made when individuals are sharing blogs publicly, especially when content is sensitive.

|  |
| --- |
| *Safety and security considerations;*   * Does the author need to be anonymised? * If so, do any details of the story need to be changed to protect anonymity? * Is the information going to be triggering for individuals who might come across it? * If so, are trigger warnings needed? * If the blog is being uploaded/used on a charity or organization's web page, what support is in place for the writer, are you going to pay them? |

Numerous blogs written by survivors of domestic and/or sexual abuse are available on the AVA website, available [here.](https://avaproject.org.uk)

**Social media forums**

Using popular social media platforms can have its benefits. Individuals who might not actively be reaching out for help or might not know what to look for are more likely to come across support if it is offered on platforms they might already be using. Despite this, it is not always possible to pre moderate or reduce risks effectively on these platforms.

Considerations should be made as to whether a non-moderated forum is fundamentally inappropriate for the user group, especially where individuals might be triggered by disclosures or perpetrators might have access. For any group who might have experiences of harm or oppression, using closed groups is an important means of filtering out any potential trolling or bullying behaviour.

|  |
| --- |
| *Safety and security considerations;*  Where individuals are able to write posts or ask questions but moderation is not possible, ground rules should be agreed within the group. This might relate to;   * Practices regarding the use of trigger warnings and content notes * Agreements on images and what can be shared * Agreement on language and terminology   *Tips for moderating platforms are presented  in section 7.* |

A blog post about setting up and moderating social media platforms, available [here.](https://www.searchenginejournal.com/how-to-moderate-a-community/338011/#close)

**Using established platforms**

There are already a considerable number of free, easily accessible and functional mediums through which to communicate with others, share information and provide support. Information relating to the safety of each platform is often contradictory. It is important for any organisation or individual using these platforms to read privacy policies and ensure they are informed as to default settings of each app, and how to adapt these settings to suit the communication it will be used for.

Below is a list of commonplace platforms used by organisations to communicate both internally, with clients/service users, and in partnership working.

**Zoom**

Zoom is a video and conferencing calling platform that can be used for both one-to-one and group video calling.

* General information on Zoom is available [here.](https://zoom.us/about)
* Information on using Zoom is available [here.](https://support.zoom.us/hc/en-us)
* Information related to privacy settings is available [here.](https://zoom.us/docs/en-us/privacy-and-security.html?zcid=3747&creative=431306240810&keyword=%2Bzoom%20%2Bprivacy&matchtype=b&network=g&device=c&gclid=CjwKCAjwwMn1BRAUEiwAZ_jnEs_KA_6sPwpyUqX9apny0aXUJ1GNBh-UokN1JqyrW2e3nKHNyJvBSxoCfXIQAvD_BwE)
* Tips on keeping zoom meetings secure are available [here](https://it.cornell.edu/zoom/keep-zoom-meetings-private-and-reduce-odds-zoombombing)
* Tips for those new to zoom are available [here](https://medium.com/wethecatalysts/getting-started-with-zoom-f9e6c96f590b)

**Microsoft teams**

Microsoft teams is a video and conference calling platform that can be used for both one-to-one and group video calling.

* General information on Microsoft teams is available [here](https://www.microsoft.com/en-gb/microsoft-365/microsoft-teams/group-chat-software)
* Training on using Microsoft teams is available [here](https://docs.microsoft.com/en-gb/microsoftteams/instructor-led-training-teams-landing-page#pivot=home&panel=home-all)
* Information on using Microsoft teams is available [here](https://support.office.com/en-gb/article/microsoft-teams-video-training-4f108e54-240b-4351-8084-b1089f0d21d7)
* Information related to privacy settings is available [here](https://support.office.com/en-us/article/teams-free-support-and-privacy-statement-9116c829-c8fa-4822-96a3-1e89b2911ba5)
* Tips on keeping Microsoft teams meetings secure is available [here.](https://www.varonis.com/blog/microsoft-teams/)

**Google meet/hangouts**

Google hangouts is a video and conference calling platform that can be used for both one-to-one and group video calling.

* General information on Hangouts is available [here](https://hangouts.google.com)
* Information on using Hangouts is available [here](https://support.google.com/hangouts/answer/2944865?co=GENIE.Platform%3DDesktop&hl=en)
* Tips on keeping Hangouts meetings secure is available [here](https://techboomers.com/t/is-google-hangouts-safe-secure-private)
* Tips for those new to hangouts are available [here](https://medium.com/wethecatalysts/getting-started-with-google-hangouts-2a4b10baa395)

**Skype**

Skype is a video and conference calling platform that can be used for both one-to-one and group video calling.

* General information on Skype is available [here](https://www.skype.com/en/)
* Information on using Skype is available [here](https://www.skype.com/en/features/)
* Information relating to privacy and security is available [here](https://support.skype.com/en/faq/FA34649/protecting-your-online-safety-security-and-privacy#encryption)
* Tips for those new to skype are available [here](https://medium.com/wethecatalysts/a-practical-guide-for-getting-started-with-skype-video-calls-4a0559c31cbd)

**Whatsapp**

Whatsapp is a cross-platform messaging app with both messaging and video calling functions.

* General information on Whatsapp is available [here](https://www.whatsapp.com)
* Information on using Whatsapp is available [here](https://faq.whatsapp.com/en/web/)
* Information relating to privacy and security is available [here](https://www.whatsapp.com/security/)

**Slack**

Slack is a business communication platform which enables multiple chats allowing companies to organize communications by channels for group discussions or private messages.

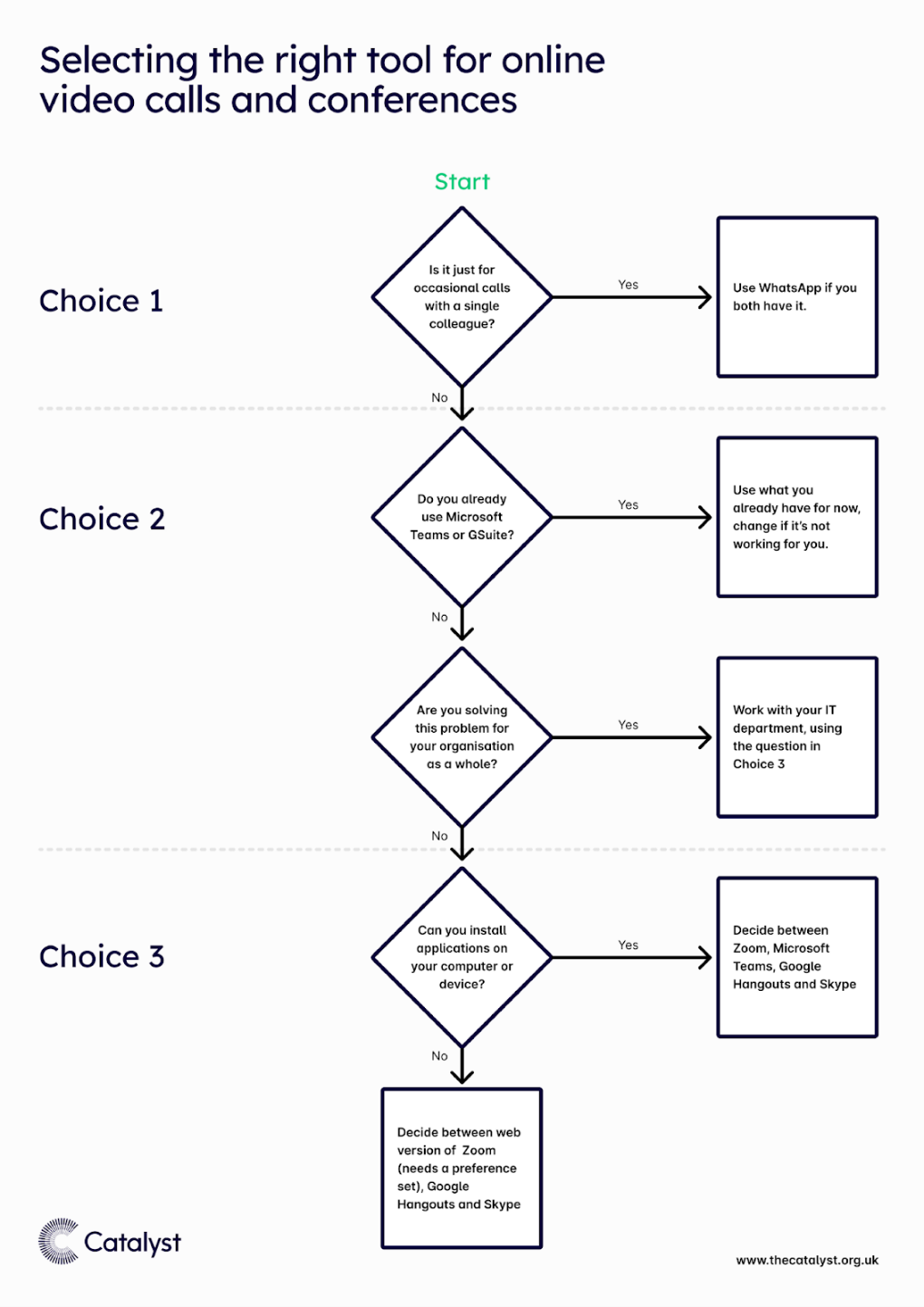
* General information on Slack is available [here](https://www.googleadservices.com/pagead/aclk?sa=L&ai=DChcSEwiwqYftsJ_pAhWmgFAGHSI4DcIYABAAGgJkZw&ohost=www.google.com&cid=CAESQeD2fnfUJrzPTf46VWydaG2Oyo15fpu4za89cy2M79BM_9c3knJLYnWfGTC8oheAE83V-1C3VokKWY5Q_C4kgq9c&sig=AOD64_2ewf5GVTCflW9jsW4ODxBy-qdt2w&q=&ved=2ahUKEwjlo__ssJ_pAhWRr3EKHSygBGcQ0Qx6BAgjEAE&adurl=&bg=!cXKlcmpYny7sWVXj9ZECAAAAU1IAAAACCgBLzkn9Waz8L7KFeqh_ES-T9WMOFFvmVJHS2TdxrJtjBDk6DRaYnuCLkT64qyMMH7XOpQVdsT3BrldbR8bXnIWIFlsfR2Scd39wcOC8mQDeEGcH8AVVHoUn5gMrwkd27UuH4tsSeMHeb2HlwGvqN21-emSifw8e1pWqGtcWuNMcvFGzXk3Vje0KUR3wBJEuTSdjbqgj4axExyj2EAi9mHOhUBFvXilROgkwB0JrTJzx8BGeC9Tvr8tlJJ05AqZ2awW25OupLjb6uhhCnrZJHfPxUqVijeJG1HhOgyR0Kxq0rVd5iIuCddFJQFFm2FVIIdiCcuosejpbSgKrEQO-YlMKbIpO8pkkWvddxLO4D2_PwGCO__xKZ9plTK8UvQKCwMDJDGaExKkyhLR3bs8h)
* Information on using Slack is available [here](https://slackdemo.com/?vst=7sezkzlnl36inawug9vrzhtyv)
* Information relating to privacy and security is available [here](https://slack.com/intl/en-gb/help/articles/202014843-Slack-data-security-and-privacy-policies)
* Tips on keeping your Slack platform safe available [here](https://slack.com/intl/en-gb/help/articles/115004155306-Security-tips-to-protect-your-workspace).

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Platform | Free to use | Pay to use functions | One-to-one and group | Calling function | Video calling function | Messaging function | File sharing | Interactive functions  (screen sharing, polling, whiteboard) | Break out function |
| **Zoom** | x | x | x | x | x | x | x | x | x |
| **Microsoft teams** | x | x | x | x | x | x | x | x |  |
| **Google hangouts** | x | x | x | x | x | x | x | x |  |
| **Skype** | x | x | x | x | x | x | x | x |  |
| **Whatsapp** | x |  | x | x | x | x | x |  |  |
| **Slack** | x | x | x | x | x | x | x | x |  |

An issue which has arisen recently is the impact of seeing your own image when on video calls. This can lead to or exacerbate **body dysmorphia** and can cause distress. It is important to find out if the platform you use allows the user to hide their own image (the rest of the group should still be able to see them, but they won’t see themselves). Make it clear to everyone that this is an option so they can make that decision for themselves.

Encrypted apps provide the greatest level of security. **Encryption** means encrypting communications in order to make information unavailable to third parties. Whatsapp is the most popular app to use end-to-end encryption making it a suitable choice for communicating with individuals around sensitive information. Further information and examples of encrypted messaging apps is available [here.](https://heimdalsecurity.com/blog/the-best-encrypted-messaging-apps/) Further information on the relative security of the key video-calling apps is available [here.](https://www.inc.com/adam-levin/zoom-webex-microsoft-teams-google-hangouts-meet-duo-security-privacy.html)

The Catalyst have created a useful diagram to assist in choosing which video calling tool works for your organisation:



(The Catalyst, 2019) - further considerations are detailed [here.](https://medium.com/wethecatalysts/selecting-the-right-tool-for-online-video-calls-and-conferences-f0e11174dbb5)

As mentioned, each app has its pros and cons and the key considerations are security and privacy, as well as useability. When working with vulnerable individuals, never substitute privacy for function, ensuring conversations are secure and safe (as they are in Whatsapp, for example) is crucial.

**5. The Differences to be Aware of When Working Online**

There are some huge differences between working face to face and working online.  These come with both challenges and opportunities and online support may be a barrier for some and an enabler for others.

Some things to be aware of include:

**The Online Disinhibition Effect**

There can be a tendency online to loosen social inhibitions, often due to the anonymity offered online. Even when someone is not anonymous, this concept still seems to occur meaning that you may find that people will disclose or share personal things much more quickly and directly than they would in a face to face setting. For some, this can be empowering and therapeutic, whereas others may share and then wish they had not been so quick to do so. Another side of this is the ‘toxic disinhibition’ effect which can lead to people posting abusive comments or bullying/trolling others.

You may want to talk to users before they engage with your service about what they share and when and it is important to have clear guidelines about unacceptable behaviour and how abusive comments and trolling will be dealt with.

Also, consider how you will feel and react to disclosures happening more quickly than you may be used to. Clinical supervision and team de-briefing will be important to help with this.

**Lack of Facial Cues/Body Language**

Even on video calls, it can be hard to assess someone's emotions. Many of the usual signs of non-verbal communication may also be lacking (such as eye contact, posture, body movement, gestures, voice etc). This may lead to interactions online feeling disjointed, remote and uncertain. Consider how you will be able to pick up on someone’s emotions and mental state if you are not able to see them, especially if the communication is asynchronous.

**Access to Technology and The Confidence to Use It**

Not everyone will feel confident using technology (both service users and staff alike). People might need training or support to use software and access the tech. How can you make sure it is accessible to everyone, equally? Some people may not have access to the devices needed or may not have wifi to access your services.

Some may have had previous experiences of using tech that were traumatic, and need reassurance and extra support. Make sure to provide clear information and transparency around the security in place, data sharing, confidentiality policies etc. Help them understand what they will experience before they do by providing training sessions.

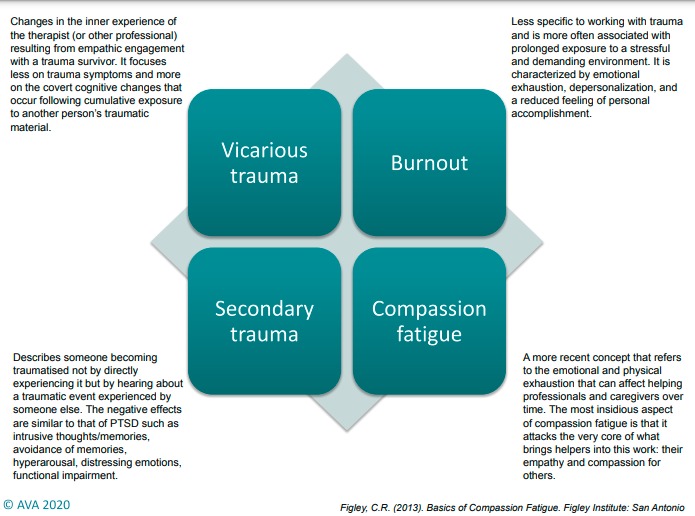
Another thing to be mindful of is how it feels to both provide and access support from within the home. Many people see home as sanctuary and safe space. Think about how it feels for you working from home, and then think about it from the users’ point of view. Do they have a safe and confidential space? Consider what they will be feeling once they have left the computer / switched off the tech. You may need to provide information on self-care, grounding exercises and provide further support information. Equally, for people facilitating work online, you may also need to debrief and consider how working online, especially with vulnerable people, will affect you.

**Open working**

A perk of working online is that you can make your processes, resources and platforms available for others to use, view and learn from - allowing you to share best practice. Lots of organisations encourage open working when creating and carrying out services online. *“Working in the open is as simple as sharing your work with others - inside or outside your organisation - and using work that’s been done by others to help you with your project.”[[13]](#footnote-12)* The aims of open working are to share learning, gain from others so you make more progress and therefore help more service users/client groups. Also, by being able to learn from ideas that already have successes and weak points documented you can save time on mistakes and in turn save money. [Read the full article here on open working.](https://www.thecatalyst.org.uk/blog/what-is-working-in-the-open-for-non-profits)  [Here](https://www.thecatalyst.org.uk/blog/how-to-work-in-the-open-sharing) is another article by Catalyst on the specifics of how to enact open working.

**Vicarious/secondary trauma, burnout, compassion fatigue**

Working with service users experiencing various forms of abuse or oppression includes the risk of professionals feeling intensely drained, anxious, unhappy and other common feelings of trauma, due to repetitive exposure and empathy for those service users. The image below details different types of trauma felt by professionals online and offline.



These effects can be felt just as intensely when working online as working face to face with a client. We know that disclosures may even happen more often with the online disinhibition effect. When designing digital solutions it is important to put in as much thought to your staff’s wellbeing as you would with face to face services. Self-care is something you should encourage your staff to prioritise but it is an organisational responsibility to protect your staff from burnout and work with them to limit the effects of secondary and/or vicarious trauma.

[Here](https://www.researchgate.net/publication/276455324_Organizational_Prevention_of_Vicarious_Trauma) is a paper on ways for organisations to prevent vicarious trauma.

AVA offers a training course called [Becoming Trauma Informed: A Course for Managers](https://avaproject.org.uk/in-house-training/creating-trauma-informed-services/) on this topic and another called [Managing The Secondary Effects of Working with Trauma](https://avaproject.org.uk/in-house-training/managing-secondary-effects-working-violence-women-girls/).

[Here](https://www.bma.org.uk/advice-and-support/your-wellbeing/vicarious-trauma/vicarious-trauma-signs-and-strategies-for-coping#:~:text=Strategies%20for%20reducing%20risk%20of%20vicarious%20trauma&text=Increase%20your%20self%2Dobservation%20%2D%20recognise,your%20physical%20and%20mental%20wellbeing.) is a good list of techniques for individuals to enact to reduce vicarious trauma put together by The British Medical Association.

[AVA’s resource hub](https://avaproject.org.uk/covid-19-resources/supporting-yourself-during-through-covid-19/) may be helpful if you are looking for self-care tips or more information on secondary trauma.

**Video call/tech fatigue**

Covid-19 may have sped up your switch to digital, but it is likely that now you are beginning to think about the possibilities or have created and are running successful services, online will become part of service delivery from now on. The combination of engaging in services or working online with people’s use of smart devices for socialising and their own digital admin and hobbies means that we are spending more time on their internet than ever. What does this mean for your services, your client groups and your staff? Put simply you need to be aware of the possibilities of tech fatigue and fight against it by keeping everyone engaged and encouraging a mix of time online and offline.

*“Video call fatigue can make otherwise content people anxious and may increase anxiety levels in those already experiencing such feelings. Video call fatigue can cause people to feel overwhelmed when they would not usually, leading to increased tiredness and even exhaustion.”[[14]](#footnote-13)*

[Here](https://www.weforum.org/agenda/2020/05/zoom-fatigue-video-conferencing-coronavirus/) is an article by the World Economic Forum on “Why video call fatigue might be making you tired during lockdown - and how to beat it”. There are many articles on this topic including from the [BBC](https://www.bbc.com/worklife/article/20200421-why-zoom-video-chats-are-so-exhausting) and [National Geographic.](https://www.nationalgeographic.co.uk/science-and-technology/2020/04/zoom-fatigue-is-taxing-the-brain-heres-why-that-happens)  Bupa has shared [5 tips to tackle video call fatigue.](https://www.bupa.co.uk/newsroom/ourviews/five-tips-video-call-fatigue)

*“Mental fatigue, memory issues, a decrease in motivation, and an increase in stress characterise technology fatigue.”[[15]](#footnote-14)*

[Here](https://www.iwgplc.com/MediaCentre/Article/tech-fatigue-why-we-need-balance-boundaries-in-workplace) is an article by the International Workplace Group on “Tech fatigue: why we need balance and boundaries in the workplace. Lots of the tips online encourage regular breaks, we encourage you to ensure this is part of your service design or company culture so that the onus is not on the individual to ask for breaks or other boundaries and self-care - we need to make sure we are designing with the risks of tech fatigue in mind.

**6. Managing Groups Online**

As explored above in relation to the setting up of forums, games and peer support platforms, creating groups online can be a brilliant means of bringing individuals together to support one another and share information. As with all digital endeavours, this can be incredibly fruitful, but in order to be successful and supportive, various risks need to be considered and mitigated.

The first step when managing groups online is to consider what platform best suits both the nature and needs of the user group (see section four). The risk of using your chosen platform should be considered, as well as the privacy and security protections in place.

Is this an established face to face group or a totally new group? If they have formed relationships already in a face to face setting you will still need to consider how they can be transferred online. If they have not met before - how will you help them to create a safe space and build those relationships?

**Top tips for setting up and managing groups include:**

|  |
| --- |
| * **Starting with a goal:** *what is the purpose of your group? Make this clear to all potential users. If you are starting from zero, ask your target group what they want to see.* * **Establish leaders or moderators:** *whether setting up the group to run independently or moderating the group, establish the hierarchies of group organisation early on and make them transparent to all group members.* * **Solicit feedback:** *create an easy feedback loop to ensure any potential changes or complaints are rectified.* * **Encourage active participation:** *encourage all members to get involved.* * Establish rules around anonymity: *make clear policies relating to the use of pseudonyms or the need for transparency. It will depend on your platform whether you think it appropriate or not for individuals to share personal information.* * **Set ground rules/group agreements:** *in partnership with relevant organisations and potential users, create and present a set of ground rules for all potential users. This might include agreements around: language, information sharing, communication style, image sharing, off-platform contact.* * **Use different activities and break out sessions:** *ensure you are keeping people engaged and appealing to different learning and communication styles.* * **Honour emotional states:** *plan on how to deal with it if someone becomes very upset (consider the use of breakout rooms). What will you do if someone does not turn up or ‘disappears?’ Discuss with the group and include this in the group agreement.* * **Debriefing:** *for both group members and facilitators to ensure people feel supported and not left feeling triggered or traumatised.* * **Equal access**: *oppression can be compounded by technology – how can you encourage active and equal participation?* |

A simple step by step guide to setting up groups online is available [here.](https://www.go2s.com/managing-a-group-online-the-ultimate-guide/)

**7. Moderating Forums**

Moderation is an activity or process following an agreed policy or set of guidelines to encourage safe and responsible use of an interactive service in accordance with the Terms of Service, Acceptable Use Policy or ‘House Rules’.

Moderation is performed by human moderators or filtering software (or a combination) reviewing content posted by users and removing content or restricting users as necessary, either pre- or post-publication in near real time or following user reports. Moderating online activity is mentioned in the [Safeguarding Vulnerable Groups Act 2006 – schedule 4.](http://www.legislation.gov.uk/ukpga/2006/47/schedule/4)

If running an online forum or enabling conversations through a different medium, moderation might be advisable. It is preferable to pre-moderate posts where possible.

|  |
| --- |
| Examples of instances where moderation may be necessary:   * Trolling, abusive and bullying behaviour * Intense and potentially triggering disclosures * Communication of personal and intimate information that may lead to someone being identified * There might be posts which need editing in order for them to be appropriate.  In this case moderators might contact individuals, letting them know what they have removed and why. |

In the case of any content that suggests risk, moderators should have clear policies in place, both in relation to contacting those who are perpetrating risk, those who are potential victims, and those who might disclose being a victim of abuse. This might include;

* Creating a flagging system for posts that present risk (of any form)
* Creating a standard procedure for removal from the forum (or non-posting), responding to the poster in question and escalating if necessary.

If the moderator believes that the individual might be at serious risk to themselves or others, they must escalate the concern. A policy must be in place in relation to what constitutes a risk, risks often take different levels of severity.

|  |
| --- |
| * High level risk: threats of suicide/self-harm, threats to harm someone else, breach of a court order, child abuse, child protection concerns, domestic abuse * Medium level risk: where you may be unsure as to whether to post a message – it may contain a discussion about services/court cases etc * Low level risk: swearing, talking about a different topic (if you just want a second opinion but there is no risk) |

Procedures should be in place to ensure each level of risk is handled correctly following a set out safeguarding pathway. Clear policies are also an important means of ensuring the comfort and safety of moderators, especially when holding high levels of risk. There are a lot of successful social media or alternative forums, most with transparent guidelines and moderation. Seek advice and identify good practice already available on pre-established platforms.

**8. Privacy and Security**

When creating or using a digital platform there are various considerations that need to be made in relation to privacy and security. Below are some key considerations and resources to aid in embedding privacy and security.

Most laws and regulations regarding privacy and security fall under The Data Protection Act (2018)[[16]](#footnote-15) and the General Data Protection Regulation (2018)[[17]](#footnote-16).

**Confidentiality**

Confidentiality in digital spaces is much the same as it is in face-to-face encounters. When working to support individuals and handling their information, confidentiality must be ensured to the highest degree. Confidentiality must only be broken where a safeguarding risk is apparent and you believe the individual to be at risk of harm, either to themselves or others.

|  |
| --- |
| *To ensure confidentiality* all information must be stored in a secure, password protected file or other secure medium. Information should not be shared with anyone outside of pre-defined (and transparent) parties. Make individuals aware of your safeguarding responsibilities and requirements to pass on information if you believe they are at risk of harm. |

|  |
| --- |
| *When breaking confidentiality,* if you have a concern, make sure you have the service user’s consent if you are passing on their information unless there are good reasons not to, for example, it is necessary to protect public safety or prevent harm to other people. |

|  |
| --- |
| *When passing forward information*, ensure the information is only shared with relevant parties and individuals and that identifying features are only included where necessary. Always inform individuals to who and where their information has been sent (where possible) and update them where relevant. |

|  |
| --- |
| *Sharing information with your team/colleagues* may be justified if you need advice or assistance. The law does not prevent the sharing of sensitive, personal information within organisations. |

A clear policy relating to confidentiality should be available to users of digital platforms and where using digital technologies. A quick guide to data confidentiality is available [here.](https://www1.udel.edu/security/data/confidentiality.html)

**Consent**

The age of consent for accessing online services in the UK is 13. Children over 16 are entitled to consent to their own treatment, this includes data protection and storage. Refer to [GDPR Article 8](https://gdpr-info.eu/art-8-gdpr/) for full guidance. If you are providing a counselling service this may not apply as it may be seen as being in the best interests of the child. Make sure to check the guidance to be clear with regards to the service you provide[[18]](#footnote-17).

When sharing information, for example, because of a safeguarding risk, always ask for consent to share information unless there is a compelling reason for not doing so. Information can be shared without consent if it is justified in the public interest or required by law. Do not ask for consent if you have already decided to disclose information in the public interest.

When creating new digital products, make consent opt-in. Never design tools where consent is opt-out or assumed, especially when working with vulnerable individuals and/or children.

When asking for consent around an individual’s data, they should be informed of what information is being collected, by whom, how and for what purpose, how it will be shared, what effect it may have, how long it will be stored, and what rights users have around their data.

A clear policy related to consent should be available to users of digital platforms.

Girl Effect’s (2018) guidance, available [here,](https://www.girleffect.org/stories/digital-safeguarding/) provides in-depth information and tips for ensuring informed consent at all stages of product development.

If you intend to use children’s personal data to offer an online service to a child then you must do a DPIA to establish whether your processing will result in a high risk to the rights and freedoms of your data subjects.

|  |
| --- |
| **Getting/ensuring consent from children:**   * Use simple and clear language * Ask for consent more than once * Ask the child’s age (try and have assurances as far as possible) to cater consent logistics and language. * Use colourful and visually appealing forms to ensure engagement * Keep forms as short as possible |

The ICO’s guide to GDPR and consent is available [here.](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/consent/how-should-we-obtain-record-and-manage-consent/)

The ICO’s guide to consent when working with children is available [here.](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/children-and-the-gdpr/what-are-the-rules-about-an-iss-and-consent/)

**Data protection**

Data protection in the UK and responsibilities falls under The Data Protection Act (2018) and GDPR (2018). This is an intricate and specific set of regulations. Every organisation should ensure they are abiding by the requirements set out in this document.

The ICO has produced a number of useful resources to assist organisations in understanding their obligations. These are available [here.](https://ico.org.uk/for-organisations/guide-to-data-protection/)

* A key resource is their data protection by design checklist, available [here.](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/)

Article 5 of the GDPR (2018) outlines the key principles relating to the processing of personal data, which are outlined [here.](https://gdpr-info.eu/art-5-gdpr/)

**Password protection**

Password protection is a crucial part of ensuring that individuals have control over access to their personal data. This includes password protecting smartphones and laptops, as well as creating passwords for access to platforms, apps and support services. Passwords are especially essential for messaging apps or platforms where individuals might be seeking help in high risk situations, or sharing sensitive personal information.

Despite this, for individuals living with a disability or cognitive disability such as dementia, authentication and password protection often presents an insurmountable barrier.

|  |
| --- |
| Web security and privacy technologies often block people with cognitive and/or physical disabilities who may not be able to:   * discern text they are required to enter and submit; * recall text or instructions they have seen or heard; * follow multi-step procedures. |

[W3C](https://www.w3.org) provide a list of possible alternatives to password protection. These include, Fast IDentity Online (more information on this [here](https://fidoalliance.org)), password-free standards, Security-token hardware devices, and easy-use password resetting tools. More information on accessible authentication and setting up alternatives to password protection is available [here.](https://www.w3.org/WAI/WCAG21/Understanding/accessible-authentication)

**Equal access**

Ensuring accessibility is essential for those developing and using digital technologies so as to not exclude people from using their products and services. Accessibility relates to both useability and content. Accessibility is ultimately about ensuring digital inclusion, making digital technologies accessible to all regardless of age, race, ethnicity, gender, sexuality, socio-economic status or location.

*When creating a website consider some of the following:*

|  |
| --- |
| * Ensure clear and structured content * Provide alt text for images * Use hyperlinks with descriptive tags for easy navigation * Use clear headers and paragraphs for easy presentation of information * Use colour carefully, consider using toned down colour palettes for websites catering to those who may have suffered from trauma. * Use diverse and inclusive images * Use simple, clear and inclusive language * Ensure the site is keyboard friendly (if designing a website) * Enable resizable text |

An introduction to web accessibility is available [here.](https://www.w3.org/WAI/fundamentals/accessibility-intro/#context)

A guide to accessible website design is available [here.](https://webaccess.berkeley.edu/resources/tips/web-accessibility)

A guide to trauma informed website design is available [here.](https://www.1800respect.org.au/live/Medibank-1800RespectCMS/media/1468/180305-webinar-presentation-final.pdf)

Fundamental to creating accessible and trauma informed platforms is including and learning from the intended user group throughout the design process.

|  |
| --- |
| **Digital Inclusion:** to ensure that everyone, regardless of gender, income or location, benefits equally from the internet and the economic and social opportunities it creates.  **Digital Citizenship:** to ensure that the web remains truly open and affords everyone the rights and information they need to participate fully in civic life  (WWWF Strategy, 2017-22, available here: <https://webfoundation.org/docs/2017/02/WF_StrategySummaryFINAL.pdf>) |

Below is an easy do’s and don’ts guide for creating accessible website design for different user groups from Home Office digital. More information on their work is available [here](https://hodigital.blog.gov.uk).

**Embedding an exit button**

If you are creating a site or platform containing sensitive information you will need to ensure users are able to quickly escape and that the website does not appear on their internet history. This is especially important for websites providing support services to those living with abuse or harm.

|  |
| --- |
| Some key considerations for embedding an exit button on your webpage/platform are:   * Bright colour so the button is visible on the screen. * Large and simple text so the purpose of the button is clear * Always in the same position on the screen, so it is easy to find quickly. * Moves up and down on the web page when scrolling so the button is always visible and in the same place. |

Embedding an exit button on the main page of a website is a crucial way to ensure the safety of your potential service users. A guide to creating a safe exit button is available [here](https://css-tricks.com/website-escape/).

**9. Useful Resources and Links**

Below are some useful resources related to digital safeguarding, abuse and managing risk.

|  |
| --- |
| **General;**   * Tech vs Abuse: [Research Findings](https://d1c4e1f2-14ed-423b-8bab-01c0ad397d8f.filesusr.com/ugd/464d6d_b465be597dee4e04b8fac09363e4ef62.pdf) * Chayn (2018) [‘Do It Yourself Online Safety’.](https://chayn.co/safety/) * Two- Part Catalyst Blog Series by Joe Roberson: **Part One**: [What a youth trip to Dartmoor can teach us about digital safeguarding](https://medium.com/wethecatalysts/what-a-youth-trip-to-dartmoor-can-teach-us-about-digital-safeguarding-ad503ae9fc51) , **Part Two**: [How to risk assess your preferred third party platform for online service delivery](https://medium.com/wethecatalysts/how-to-risk-assess-your-preferred-third-party-platform-for-online-service-delivery-d4909c10e0a4) * Girl Effect: [Digital Safeguarding Tips and Guidance](https://prd-girleffect-corp.s3.amazonaws.com/documents/Digital_Safeguarding_-_FINAL.pdf) * Get Safe Online [website](https://www.getsafeonline.org/business/) * GDPR and Safeguarding [legislation](https://www.legislation.gov.uk/ukpga/2018/12/pdfs/ukpga_20180012_en.pdf) * The Catalyst [articles and resources](https://medium.com/wethecatalysts/viewpoints/home) assisting charities with digital development |

|  |
| --- |
| **Online Abuse;** information   * [AVA resources page](https://avaproject.org.uk/resources/) and their '[Technology and Violence Against Women Good Practice Briefing](https://avaproject.org.uk/wp-content/uploads/2019/04/Tech-and-Abuse-Good-Practice-Briefing.pdf)' * [SafeLives Digital and Online Safety page](https://safelives.org.uk/tech-vs-abuse) and their '[Staying safe online guide](https://safelives.org.uk/sites/default/files/resources/Staying%20safe%20online%20guide.pdf)’ * Women's Aid guide to '[cover your tracks online](https://www.womensaid.org.uk/cover-your-tracks-online/)' * Refuge [Tech Abuse page](https://www.refuge.org.uk/our-work/forms-of-violence-and-abuse/tech-abuse-2/) * [Tech safety](https://www.techsafety.org) website * Love is Respect’s [‘What is Digital Abuse’ guidance](https://www.loveisrespect.org/pdf/What_Is_Digital_Abuse.pdf) * UKCCIS’s guide to responding to [sexting in schools and colleges](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/759007/6_2939_SP_NCA_Sexting_In_Schools_FINAL_Update_Jan17.pdf) |

|  |
| --- |
| **Example digital safeguarding strategies (examples)**   * Cambridge and Peterborough Safeguarding Children’s Board (2018-20): [Online safeguarding strategy](http://www.safeguardingcambspeterborough.org.uk/wp-content/uploads/2018/06/Online-Safeguarding-Strategy-2018-20.pdf) * Becta: [Safeguarding Children in a Digital World.](https://dera.ioe.ac.uk/7372/2/A9R40BD_Redacted.pdf) |

|  |
| --- |
| **Web accessibility resources (from the Web Accessibility Initiative):**   * For an introduction to accessibility requirements and international standards, see [Accessibility Principles](https://www.w3.org/WAI/fundamentals/accessibility-principles/). * To understand some common accessibility barriers from the perspective of testing, see [Easy Checks – A First Review of Web Accessibility](https://www.w3.org/WAI/test-evaluate/preliminary/). * For some basic considerations on designing, writing, and developing for accessibility, see [Tips for Getting Started](https://www.w3.org/WAI/tips/). * When you’re ready to know more about developing and designing, you’ll probably use resources such as:   + [How to Meet WCAG (Quick Reference)](http://www.w3.org/WAI/WCAG21/quickref/)   + [Web Accessibility Tutorials](https://www.w3.org/WAI/tutorials/) * For project management and organizational considerations, see [Planning and Managing Web Accessibility](https://www.w3.org/WAI/planning-and-managing/). If you need to make quick fixes now, see [Approaches for Interim Repairs](https://www.w3.org/WAI/planning/interim-repairs/). |

|  |
| --- |
| **Reporting abuse;**   * You can anonymously and confidentially report child sexual abuse content, criminally obscene adult content and non-photographic child sexual abuse images via <https://www.iwf.org.uk/> * If someone has been a victim of revenge pornography, this helpline can provideadvice and get images removed <https://revengepornhelpline.org.uk/> * Reporting indecent or offensive content on Twitter <https://support.twitter.com/articles/15789> * Reporting indecent or offensive content on YouTube <https://www.youtube.com/intl/en-GB/yt/about/policies/#reporting-and-enforcement> * Reporting indecent or offensive content on Facebook <https://www.facebook.com/help/contact/274459462613911> * Reporting indecent or offensive content on Instagram <https://help.instagram.com/519598734752872> * Hate crime including online content can be reported via [www.report-it.org.uk](http://www.report-it.org.uk) * Harmful or upsetting content can be reported to <https://reportharmfulcontent.com> * If you have been the victim of fraud contact <https://www.cifas.org.uk> * If you wish to report any form of cybercrime contact [www.actionfraud.police.uk/](http://www.actionfraud.police.uk/) |

**Notes:**

1. Technology Safety [Homepage](https://www.techsafety.org/) [↑](#footnote-ref-0)
2. Raftree, L., 2018. *Digital Safeguarding Tips And Guidance*. [online] London: Girl Effect. [↑](#footnote-ref-1)
3. The Catalyst (2020) have created some tips for involving service users remotely, [here.](https://medium.com/wethecatalysts/six-ways-to-involve-your-users-in-shaping-your-new-digital-delivery-when-you-cant-go-and-meet-f026e82cee28)  Ayemind (2016) does a considerable amount of co-production work with young people, more information is available [here.](http://ayemind.com/category/co-design/) [↑](#footnote-ref-2)
4. DigiSafe 2020 - [Assess risk section](https://digisafe.thecatalyst.org.uk/chapters/assess-risk) [↑](#footnote-ref-3)
5. Digital self-harm is a form of self-aggression that involves anonymously posting hurtful and sometimes abusive remarks about one’s self online.(<https://psychcentral.com/lib/what-is-digital-self-harm/>) [↑](#footnote-ref-4)
6. Comic Relief (2017) [Tech Vs Abuse: Research Findings](https://d1c4e1f2-14ed-423b-8bab-01c0ad397d8f.filesusr.com/ugd/464d6d_8e401d0e666a4e66b1180ebc29826f06.pdf) [↑](#footnote-ref-5)
7. Women’s Aid [What is Coercive Control? webpage](https://www.womensaid.org.uk/information-support/what-is-domestic-abuse/coercive-control/) [↑](#footnote-ref-6)
8. Amnesty, 2017, [Unsocial Media: The Real Toll of Online Abuse against Women.](https://medium.com/amnesty-insights/unsocial-media-the-real-toll-of-online-abuse-against-women-37134ddab3f4)  [↑](#footnote-ref-7)
9. University of Bedfordshire, 2011, [Cyberstalking in the United Kingdom.](https://paladinservice.co.uk/wp-content/uploads/2013/12/ECHO_Pilot_Final-Cyberstalking-in-the-UK-University-of-Bedfordshire.pdf) [↑](#footnote-ref-8)
10. Emma Short, staying safe Online; [the truth about cyberstalking.](https://sigbi.org/st-albans-and-district/files/Cyberstalking-Presentation.pdf)  [↑](#footnote-ref-9)
11. Essential Digital Skills Framework, 2018. UK Gov’t 2018 available here: <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/738922/Essential_digital_skills_framework.pdf> [↑](#footnote-ref-10)
12. A Summary - Online Harms White Paper, 2019. Uk Gov’t available here: <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/811923/EASY_READ_Online_Harms_White_Paper.pdf> [↑](#footnote-ref-11)
13. Catalyst, [What is working in the open for non-profits?](https://www.thecatalyst.org.uk/blog/what-is-working-in-the-open-for-non-profits) [↑](#footnote-ref-12)
14. Medical News Today, [What is video call fatigue?](https://www.medicalnewstoday.com/articles/video-call-fatigue#effects) [↑](#footnote-ref-13)
15. Lepage Associates (solution based psychological and psychiatric services), [Technology Fatigue: What is it and how to deal with it](https://lepageassociates.com/technology-fatigue-what-it-is-and-how-to-deal-with-it-part-one/#:~:text=Mental%20fatigue%2C%20memory%20issues%2C%20a,symptoms%20resulting%20from%20the%20stress.)  [↑](#footnote-ref-14)
16. The Data Protection Act. 2018. UK Gov’t. Available here: <https://www.gov.uk/data-protection> [↑](#footnote-ref-15)
17. General Data Protection Regulation. 2018. European Parliament. Available here: <https://gdpr-info.eu> [↑](#footnote-ref-16)
18. <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/children-and-the-gdpr/what-are-the-rules-about-an-iss-and-consent/> [↑](#footnote-ref-17)