Digital Youth Work in an Online Setting

Guidance

Produced by the National Youth Agency
Version 1.0 | March 2025

Digital Youth Work in an Online Setting

Welcome to the Digital Youth Work in an Online Setting guide. This resource is structured into three key chapters, covering an introduction to digital youth work, data protection, and safeguarding and risk management in online spaces. Additionally, you will find a glossary, recommended readings, and appendices, which are referenced throughout the guide for further support.

This guide provides points to consider before, during and after the delivery of digital youth work online. This delivery could be through online meeting platforms such as Zoom, gaming spaces such as Roblox, or chat server spaces such as Discord.

This guide should be used alongside your organisation's own policies and procedures.

Digital youth work online is a setting as any other youth work setting.

What is Digital Youth Work and Digital Youth Work Online?

Digital youth work involves the use of digital technologies and spaces to connect with, engage with, and support young people. It is the process of actively incorporating digital activities, tools, and topics into youth work services.
Digital youth work online means the use of the internet in hosting and delivering digital youth work activities. Examples include:

- Delivery of a young carers group through the online game Roblox
- Hosting an LGBT+ Youth Group through the chat server Discord
- Using VR technology to facilitate a county-wide social action group
- Delivering an emotional wellbeing project with home educated young people through the online meeting platform Zoom.

Ultimately, any youth work that involves the internet is online digital youth work. This includes using WhatsApp to communicate with young people or using online meeting platforms such as Zoom and Teams.

What do I need to do when planning for Digital Youth Work Online?

Most youth workers have had some form of online interaction with young people, whether that be sending an email to a young person or hosting one to one or group sessions online during the covid pandemic.

However, when starting any new piece of youth work there are specific considerations that must be made, and this is just as important when working online as in any other youth work environment. The following considerations will assist you with your digital youth work planning.

Be led by young people:
All methods and approaches of youth work delivery should be informed by the needs of young people. You should have conversations with young people to understand the places and spaces in which they would like to see youth work, and ensure considerations and support is available to those with barriers to tech and tech knowledge.

Digital wellbeing and safety at the core:
All youth work practice and delivery regardless of place or space should be considerate of the current needs and issues faced by young people along with a clear understanding of additional risks in the digital space including online harms. Digital Youth Work should be underpinned by sound digital wellbeing and safety knowledge, and digital approaches must be thoroughly risk assessed.

Explore, trial and test online platforms and tools:
Research the platform, tool or space that you intend to use and understand any presenting risks. Test it with colleagues and decide which platform or online tool is best for your delivery. It needs to be fit for purpose so spend time testing it out and trialling with colleagues. The guide explores platforms in more detail within the data protection chapter

Keep up to date with training and CPD:
High quality digital youth work requires a digitally active workforce. Being trained, competent, and confident will enable you to actively deliver using digital tools and technologies.

Find your networks of support internally and externally:
The world of digital is pretty huge and complex, so make sure to get support from those around you. Whether that be from your data protection officer internally, or joining any digital networks, there are lots of people with the range of skills needed to deliver safe and impactful youth work digitally. Connecting with them will help you on your digital journey.

Source your resources:
There are many great guides, tools and tips available to support digital delivery. From the Digital Youth Work Resource Hub https://digitalyouthwork.scot/ to CAST's free charity resources: https://www.wearecast.org.uk/our-work/free-digital-resources/ and SWGfL's Online Safety ones: Safety and Security Online | SWGfL There is bags lots of information out there, dig and you will find it.

Be prepared for change and future ready:
Technology is evolving rapidly, and often young people understand and embrace that technology quicker than the professionals working with them. For youth work to remain responsive to their needs it is essential that you remain up to date with digital trends. This may be through having regular open conversation with young people about their digital interests or exploring tools such as the Gartner Hype Cycle which may help you understand what new tech is on the horizon. See Gartner Hype Cycles, Explained

Get permissions:
Any online platforms or tools you use should always be approved for use by your organisation before creating any accounts and undertaking any delivery. Always keep your organisation informed of what spaces young people would like to see youth work happen in, and make sure you have the appropriate permissions before setting up and delivering any work digitally.

Data Protection

This chapter is to support you to navigate data protection in digital youth work practice and help you prepare for any digital youth work you are considering delivering. The information below will help ensure that you are processing data lawfully when working with young people's information and data. However, digital youth work delivery must also be underpinned by your organisation's policies and procedures.

Prior to working through this document, we recommend you explore these key laws to underpin your knowledge and learning:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018 (DPA 2018)

Above all: Don't panic and **Take Time to Think!** Data protection rules are there to help you think about your communication with or about young people. This can take a little bit of practice, and so being more diligent and taking time with our digital interactions can really help us consider what could go wrong and mitigate against risk.

Are you familiar with The Children's Code: what is it? | ICO and the Online Safety Act: explainer - GOV.UK?

Young people's information is classified into two types of data: Personal and Special (sensitive). Both need care and attention; however sensitive information may have additional risk. Thinking about what we are doing from the very get go can help.

What is Personal and Sensitive data?

Personal data refers to any information that can directly or indirectly identify an individual, such as their name, address, phone number, or date of birth.
Sensitive data is data that is more private and requires extra protection, including:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Health
- Sex life or sexual orientation

Safeguarding disclosures and concerns for well-being are also classed as sensitive data.

For further guidance please always seek advice and support from your organisation's Data Protection Officer (DPO) and the Information Commissioner's Office (ICO)

Good data security begins with our habits: **Start with good technology hygiene**

- Don't leave your digital device or digital youth workspace unattended. If you are working with young people digitally, ensure that your screen is not visible to anyone that doesn't have permission to view the information.
- Lock your device or space the moment you need to walk away from it.
- Password or link protect your digital space, ensuring that your device or space does not allow logins other than you or those with permissions.
- Keep your passwords safe: Use an organisation approved password vault for your passwords where necessary.
- Make sure that your devices are kept up to date with cybersecurity software and always install the latest operating system updates as recommended by your organisation.
- Make sure that antivirus software as recommended by your organisation is installed on computers that you use to communicate with and about young people
- Enable multi-factor authentication when logging into spaces. This means using a second form of identity verification in addition to a password.
- When working remotely, ensure that Wi-Fi / VPN connections are trusted and be aware of data that is passing through hosted services.

Youth work can be conducted in any number of spaces and places, if you are using Wi-Fi and / or a VPN connection, you must be aware that data may be visible to hosted service providers.

Know your platforms

If young people have shown an interest in engaging with you in a digital space, take the time to understand the platform. Just as you wouldn't work with a young person in an unfamiliar physical environment, you should explore the platform alongside colleagues. Learn how to navigate it, research its features and risks, and consider the following:

- Do young people want youth work to take place in this space?
- What data will be used, and how will it be managed?
- Is there a reasonable and measurable risk in using this space?
- Can you provide a safer alternative?

Before using any online platform, ensure it is approved by your organisation. Assess its suitability by checking its age rating, testing its functionality, and, where appropriate, undertaking training. Work with other youth workers who use the platform and trial it with colleagues to ensure it is fit for purpose.

Want a template checklist to guide you through signing up for a new digital platform or tool? Check out appendix 5.

Get the right support in place

Understanding data and risk should not be one individual's responsibility alone. Once you know your platform and your rationale for using it, then find the appropriate support in your organisation to effectively assess it. This may come from your line manager or colleagues but should always include a Data Protection Officer to support you. Furthermore, utilising networks and understanding which organisations may already be using the tools or space could help inform how you safely and effective use it.

Undertake a Data Protection Impact Assessment (DPIA):

It is important to undertake a DPIA (See Appendix 1: What is a DPIA?) whenever you are introducing new technologies or systems to your youth work practice. It is also extremely important when using existing technologies or digital tools that you review your existing DPIA's to ensure that the technology has not gone through any significant changes, and to check if there has been any significant change to guidance due to law or a breach.

For more information, please visit the Information Commissioners Office Website:
Information Commissioner's Office (ICO)
Template DPIA: dpia-template.docx (live.com)

Monitor and review Privacy and GDPR Policies:

Platforms regularly update their policies; make sure these updates have been checked and recorded in your DPIA.
If you/ your service is developing a new digital space or service, you may need to develop and present your own privacy statement independent of these platforms.

Keep a master monitoring record of the platforms you are using:

This can be done by creating a spreadsheet of all the platforms, apps and software that you use, and creating columns to show that you have read the T&C's, privacy notices, and understand the risks (which should be reflected in your risk assessment). This information should include the date checked and the date of the most recent T&C updates.

Record sessions only when necessary:

Do you have a specific, explicit, and legitimate reason for recording? Recording should not be a default position, especially if you would not have recorded a face-to-face session. Do not consider recording as a replacement for appropriate safeguarding, and ensure you refer to relevant DPA 2018, GDPR (EU and UK) guidance if you are choosing to record a session or save a transcript.

A **transcript** refers to a written or typed document that provides a detailed and accurate account of the spoken words captured during a recorded session. It may include text, timestamps, speaker labels, and sometimes additional notes on tone, pauses, or context, depending on the level of detail required. This must also be added in the DPIA under storage options, and you must write a retention policy describing how long and where the recordings will be stored safely and securely. Organisations are also responsible for having their own Data Retention policy. You can learn more here: Retention and destruction of information | ICO.

Participation and Consent: Transparency is Key

When using new platforms, be transparent with young people and support them to check and adapt their privacy settings, understanding what data will be used or shared by the organisation and the platform provider. Share this information with parents and guardians as part of the consent process and share that they have the right to request a copy of any information held through a Subject Access Request. A guide to subject access | ICO

- Make sure that young people, their parents, and guardians are aware of the platform you are using and why you are using it. Make sure that it is easily understandable with a clear explanation of the piece of work you are undertaking with the young people and provide information on the platform being used.
- Be open about risks and safeguards involved, everything should take into account the best interests of the young person. Be aware of less obvious risks such as cookies!
- Have a data protection impact assessment and data protection statement that you can share with a young person, their parents and carers before gaining their consent (refer to what is a DPIA).
- Obtain explicit consent from participants or their guardians if under 18 for data collection and use and keep a record of this.

Did you know? Websites use cookies to track your online activity, storing data such as login details and browsing habits. While they enhance user experience, some cookies can also collect personal information raising privacy concerns! (See Appendix 2 Get to know Cookies!)

Regardless of whether the young person already has an account set up with your chosen platform e.g. Roblox, Discord, or Zoom, it is still important that they and their parents or carers are informed, aware, and consent.

Digital Age of Consent

The digital age of consent in the UK is 13. This means that if you are planning to deliver a digital programme either online or offline that requires a young person to register or sign in to an account with their own details, then they must be aged 13 or over. In addition, you must obtain parental consent in line with your organisational policies.

Data Breach A data breach occurs when sensitive, confidential, or protected information is accessed, stolen, or exposed without authorisation.

Data breaches are more common than people think, and affect individuals, businesses, and governments worldwide. That's why strong passwords, multi-factor authentication, and security awareness are crucial for protecting your data and that of young people. They can happen due to:

Cyberattacks Hackers exploit security vulnerabilities to steal data.
Human Error Employees accidentally leak or expose data.
Weak Passwords Easy to guess passwords make accounts vulnerable.
Phishing Scams Fraudulent emails trick people into giving up credentials.

Safeguarding

Online digital youth work should be delivered in well managed and risk assessed spaces through clear guidance, policies, processes and boundaries, offering safer alternatives. Youth workers should be trained to engage young people in online spaces through tried and tested platforms.
This chapter is to support you to navigate and implement appropriate safeguarding measures in digital youth work practice, helping you to prepare for any digital youth work you are considering delivering.

At the forefront of any of our work in the digital and online space, safeguarding is paramount and as with any other form of youth work delivery, it should be undertaken with careful consideration of the risks in these spaces.

If you deal with online situations in the same manner as you would offline, off platform, and in the real world then you will be taking the best course of action to support the young people you work with. Given the small amount of direction about digital safeguarding in Working Together legislation you may feel overwhelmed with the number of harms children can encounter but remember that you are trained to recognise risk and manage disclosures: in the online and digital spaces it really is no different.

As a starting point: Your safeguarding knowledge and fundamentals are always your baseline when working in digital spaces. Your safeguarding knowledge and skills transition with you in digital spaces and you will handle any safeguarding concerns as you would in face-to-face settings - you may just need to consider some of these steps when preparing to work in digital spaces and think about how you would handle risk and/or concerns in digital spaces should they present.

Assessing Online Risk

Young people face varying levels of risk online, depending on their activities and the spaces they frequent. By using your judgment and engaging in open conversations, you can gain a clearer understanding of their online behaviour and the environments they navigate. This insight will help you assess the level of risk and determine how best to support them in these digital spaces.

Experience Considerations:

- Why do young people like using these tools or platforms and what is their usage?
- Have young people experienced online bullying or harassment in these spaces and environments?
- Have young people been exposed to illicit content/ material in these spaces?
- Have the spaces had a negative or detrimental impact on their wellbeing?
- Can they be sent voice or personal messages in these platforms or spaces, if so what kind of messages are they receiving and what is said or asked?

Content Considerations

- Is the platform age-appropriate?
- Is there a risk of accessing adult or extremist material?
- Have young people reported seeing abusive, racist, homophobic, sexist, or violent content?

Practical Questions:

- Do young people want youth work to take place in these spaces?
- Are you creating additional risks by using certain platforms?
- Can you provide a safer alternative?

As in the chapter before ensure you have a strong understanding of the platform or tool you are using, including its features, risks, and safety settings. Research its age rating, test it with colleagues, and consider training if needed. Just like a physical youth work space, take the time to familiarise yourself with the environment to ensure it is safe and suitable for young people.

Complete a risk assessment:
Undertake a thorough risk assessment at least two weeks before the planned activity to be agreed and signed off by your line manager, considerations should be made for: What platform you are using, it's age rating, registration and verification process, responding to disclosures, staffing ratios, IT failure, data privacy compliance, accessibility for all participants, emergency contact procedures, and any additional risks specific to the activity or audience involved. Ensure that all relevant team members are informed of the risk assessment and understand their roles and responsibilities. For further guidance please check the links below.

👋🏻 Welcome to DigiSafe | DigiSafe (thecatalyst.org.uk)
Keep Children Safe Online: Information, Advice, Support - Internet Matters

Emergency Contacts and Location Information:
As part of your consent process (highlighted in the Young People section) make sure to get emergency contact information for young people and keep this regularly updated. You must also find out where people plan to be when you deliver the session and capture this on the register/ contact emergency information. This means if an urgent risk arises, emergency services can attend the right location.

Consider how many facilitators or moderators you need:
You might want to think about roles, ratios, breakout rooms where applicable, how interactive the session is, but also someone on standby in case you lose connectivity or there is a safeguarding incident. Youth work online should never be delivered solo and generally a minimum of two mitigates against most risks.

Have a DSO on call:
Make sure you have a Designated Safeguarding Lead or Officer on call for your online event in case you need to escalate a concern, also make sure they can access the online space if necessary for example sharing with them the zoom meeting link or gaming space.

Have an age verification process in place:
Once young people are registered factor time in advance to verify that they are who they say they are, this could be by asking some questions around their age, where they go to school/ college and have a visual arrangement - this could be done in person or via videocall.

Only deliver online youth work in lockable spaces:
Online sessions in a gaming, meetings space or chat server for example should only be accessible by password and not open to the public. Do not advertise the session link and password publicly and only share the password or access link with the young people registered.

With many platforms and accounts, you can control features and even disable them to make it safer for young people. Make sure to include these choices in your Risk Assessment and Data Protection Impact Assessment detailing why you are using/disabling certain aspects of the platform.

Control considerations should include:

- **Creating a private space -** Most platforms and spaces allow for the creation of a private and or password protected space, online youth work should not be delivered in publicly accessible digital spaces.
- **Waiting Room -** Create a waiting area for those joining, so you can check and ensure they are the young people you are expecting before letting them in. You should enable this feature to prevent unexpected people entering the call.
- **Private Messaging -** disable private messaging in your settings if you do not want participants talking to each other privately but ensure young people are able to directly message you as the host.
- **Screen Sharing -** disable screen sharing to only allow the host to screen share during the session.
- **Moderation -** If using a chat server space for example, make sure to have moderators available in the space to maintain the safety of young people and definition of roles.
- **Set opening hours -** If using a platform such as a gaming or chat server space ensure open and closing hours are in place so that the space is not operating unsupervised.
- **Code of Conduct -** An agreement in place with young people setting out what we are doing in the space and how we will appropriately use it.

Ensure that age ranges and group numbers of young people are appropriate for the online session. You might want to think about delivering two separate sessions if you have a wide age range or a large number of young people.

Be considerate of screen time.
You will lose young people if the online session is too long or does not have regular breaks. Think about the age range, try to make screen-based sessions a maximum of 1 hour. Consider breaks and be creative with the most engaging ways to deliver online.

Procedures
Ensure all Youth Workers understand organisational policies and procedures. Always have up to date location information for young people and emergency contact information to hand, always have a minimum of 2 members of staff on the call, so that if a disclosure is made you can appropriately allocate actions and signpost where necessary.
Inform your DSO when your session has ended.

Be contactable:
Ensure there is a way for young people to contact you or a colleague online or offline, whilst the online sessions are taking place should they have any concerns or need support.

Handling Digital Disclosures:
Digital disclosures occur when someone shares sensitive or concerning information online or through a digital platform. This could include- emails, an online meeting, video calls, or other forms of virtual communication. You must adhere to safeguarding protocols to ensure safety, wellbeing and privacy of the individual. (See more on key guidelines in Appendix 3)

Examples of digital disclosures

- A participant in a webinar privately messages a facilitator to disclose experiences of abuse.
- A young person shares concerns about bullying through a chat feature during an online class.

Guidelines for delivering safer and inclusive online sessions

Consent forms:
Treat online youth work like you would face-to-face. Parents have legal parental responsibility for their children up to the age of 18 so involving parents and making them aware of the platforms or tools you are using wherever possible is good practice making sure they and the young people are aware of what platform is going to be used, how and how information will be shared.

Ensure young people can access the platform you're using:
As mentioned above the digital age of consent is 13 and any digital platforms that require personal data for sign up should not be used by young people under 13. Make sure young people taking part understand the programme, platform or software and know how to download and use it. Make sure they've had plenty of time to create an account or support them to find a solution.

Thinking about young people's needs:
To ensure the space is as inclusive as possible, ask if young people have any specific requirements, such as subtitles, screen readers, colour contrast settings, or alternative communication methods. Being online does not automatically mean a session is accessible, and digital spaces can present barriers for some disabled young people.

Familiarise yourself with the accessibility features available on the platform you're using and ensure they are enabled where needed. If possible, offer multiple ways to engage, such as text-based chat, audio, and video options. Encourage young people to share any additional support they may need and adapt your delivery to accommodate a range of needs, including sensory sensitivities, mobility impairments, and neurodivergent communication styles.

Ensure you have sent through any online guidance to young people who are attending:
This should help them access the space, organise anything they need to prepare for beforehand e.g. confidential space and support them in knowing what is expected of them and others in the digital environment. This might include a code of conduct. An example code of conduct or a group agreement can be found in Appendix 4

Before the session begins, take the time to familiarise participants with the platform's features, accessibility options, and any relevant guidelines. This will help create a smooth and inclusive experience, ensuring that everyone feels confident and prepared to engage fully.

Before the online session starts:

Re-check and test your settings, log into the platform early to run a test with colleagues.

Be identifiable If you have an **ID** or uniform that would be visible on screen (if applicable), please wear this and add a branded screen background where necessary. If using gaming or chat server spaces make sure it is clear you are a youth worker in your screen name ie Joe Bloggs- Youth Worker.
If using an online meeting platform close other browsers or other documents so that if you end up **screen sharing only the appropriate files** are up and you are not going to screen share any confidential or inappropriate information. This includes turning off notifications and pop ups.

Have a neutral screen space: If using a camera, it should not be looking into youth workers personal spaces. Use your organisation branded background or you can blur your background. Also advise young people to apply background affects.

Have your register of those that have signed up and /or sent their consent forms through accessible at all times.

During the online session:

Only allow registered participants onto the online space. This will also give confidence to the other participants that only screened and approved users are in.

Confidentiality and Safeguarding Remind young people that the online space is a safe space but as with any other form of youth work remind them of the limitations around confidentially should a safeguarding concern arise. Ensure that young people know how to raise or share a concern and follow your safeguarding procedures should a disclosure be made.

If someone leaves the space unexpectedly have a **process in place** for contacting them and re-admitting where necessary.

Use professional, appropriate language on calls, just like you would in a face-to-face session always maintaining professional boundaries. Also adding on a branded or blurred background if using video call functions.

Establish the etiquette and online etiquette e.g. cameras on / off, use of phones and chat or direct message functions etc, for the session and co-produce your agreement (code of conduct) for the session. Ensure young people are also aware of how to contact you should an issue arise during a session.

Post session:

Ensure the platform or tool is closed appropriately including closing access to the space and ending the session

Document any safeguarding issues, or signposting, appropriately and report to the Designated Safeguarding Lead in line with your organisational policies and procedures.

Depending on your project, **follow up with the project partner or client** on how the online session went and highlight anything that they should know about.

Glossary

Cyber
Cyber refers to anything related to computers, the internet, and digital technology, including online activities, systems, and security.

Cyber resilience
The capacity of an organisation or individual to prepare for, respond to, and recover from cyber threats, minimising damage and ensuring continuity of operations even after an attack.

Cyber Security
Cybersecurity is the process of protecting computers, networks, and data from unauthorised access, attacks, or damage

Data
Data is information collected, stored, or processed.

Data Protection Officer
A Data Protection Officer (DPO) is a professional responsible for ensuring an organisation complies with data protection laws.

Data subject
An individual whose personal data is being collected, stored, and processed by an organisation, typically with specific rights regarding the control of their personal information under data protection laws.

Digital
Refers to electronic technology that generates, stores, and processes data. It encompasses anything involving computers, networks, or online environments.

Digital wellbeing
The state of maintaining a healthy and balanced relationship with technology, ensuring it enhances rather than detracts from mental, emotional and physical health.

Discord
Discord is a digital communication platform designed for text, voice, and video chatting.

Gaming
The practice of playing digital or video games, either online or offline, using various devices such as consoles, computers or mobile phones. Popular games include Fortnite, Minecraft and Roblox.

GDPR
GDPR (General Data Protection Regulation) is a European Union law that protects personal data and privacy by regulating how organisations collect, store, and use people's information.

Multifactorial Authentication (MFA)
MFA (Multi-Factor Authentication) is a security process that requires users to verify their identity using two or more authentication factors, such as a password and a code sent to their phone.

Offline
The state of being disconnected from the internet or a network. In terms of youth work, this references the use of technology in physical settings.

Online
The state of being connected to the internet or a network, enabling access to digital resources, websites, social media and other internet-based services in real-time. In terms of youth work practice, this references the use of the internet.

Online harms
Online harms refer to harmful activities or content encountered on digital platforms, such as cyberbullying, misinformation, exploitation, or privacy breaches.

Online safety involves protecting individuals from risks and harms on digital platforms through secure practices, policies, and technologies.

Roblox
Roblox is an online platform where users can play, create, and share games

Synthetic media
Synthetic media refers to content created or manipulated using artificial intelligence, such as deepfakes, AI-generated images, videos, or audio, often designed to mimic or alter reality.

Verification
Verification is the process of confirming that something is true, accurate, or valid.

Virtual reality (VR)
A computer-generated, immersive environment that users can interact with through specialised equipment, such as VR headsets, creating the sensation of being present in a digital space.

Further reading and resources

- NYA Practice Standards - Raising the bar – Youth Work Practice Standards
- NYA Safeguarding Standards
- NYA Digital Youth Work Standards
- Youth Participation Framework - Hear by Right
- European Guidelines for Digital Youth Work
- National Occupational Standards
- Digital Youth Work - A Finnish Perspective
- Screenagers Guidance for Digital Youth Work
- Guidelines for Digital Youth Work
- Developing Digital Youth Work - Policy recommendations training needs and good practice
- Digital Youth Index
- Digital Youth Work resource hub

Data Protection

- Children's Code Strategy progress update
- Information Commissioner's Office
- General Data Protection Regulation (GDPR) – Legal Text

Appendix 1

What is a Data Protection Impact Assessment (DPIA)
A DPIA is a tool used to identify, assess and mitigate data risks in the use of digital technologies.

A DPIA is described by the ICO as being:

....a process designed to help you systematically analyse, identify and minimise the data protection risks of a project or plan. It is a key part of your accountability obligations under the UK GDPR, and when done properly helps you assess and demonstrate how you comply with all of your data protection obligations.

It does not have to eradicate all risk, but should help you minimise and determine whether or not the level of risk is acceptable in the circumstances, taking into account the benefits of what you want to achieve.1

When should I undertake a DPIA?
In Digital Youth Work it is important to undertake a DPIA whenever you are introducing new technologies or systems to your youth work practice, it is also extremely important that when using existing technologies or digital tools that you review your DPIA's to ensure that the technology has not gone through any significant changes or if there has been any significant change to guidance due to law or a breach.

Why should I undertake a DPIA
The purpose of a DPIA is to Identify Risks and enables you to assess the potential impacts on the privacy and data protection rights of young people and your organisation. It also enables you to Mitigate Risks and implement measures to minimise identified risks. Finally, it Ensures Compliance and enables organisations to demonstrate adherence to data protection laws and principles.

Who should undertake a DPIA?
A Data Protection Impact Assessment should be completed in conjunction with the organisations Data Protection Officer (DPO) or a designated individual within the organisation who has expertise in data protection and privacy. In some cases, a youth worker may be asked to initially work on a DPIA but the final review and sign-off of this document should be the person responsible in the organisation for data protection again such as a data protection officer.

Please note: While it is important to have the DPO approve and sign-off the DPIA, it is the individual introducing the new technology / platform to "complete" the DPIA

<u>Data Protection Impact Assessments (DPIAs)</u>

Appendix 2

Get to know Cookies!
What Are Cookies?
Cookies are small text files that websites store on a user's device (e.g. computer, phone, or tablet) when they visit a website. They help websites remember user preferences, login details, and browsing behaviour. Cookies can be categorised into:

- **Essential Cookies** Necessary for a website to function properly.
- **Analytical Cookies** Track user behaviour for insights and improvements.
- **Functional Cookies** Enhance user experience by remembering preferences.
- **Advertising/Tracking** Cookies Used for targeted ads and profiling.

Negative Impacts & Challenges
- **Privacy Concerns** Tracking cookies can collect personal data, raising ethical and legal issues.
- **Consent & Transparency** Youth workers must ensure compliance with GDPR and other privacy laws when handling young people's data.
- **Digital Literacy** Young people may not understand cookies' implications, making digital literacy training essential.
- **Targeted Advertising Risks** Behavioural tracking can expose young people to inappropriate or manipulative advertising.

Best Practices for Digital Youth Workers
- **Educate young people** about cookies, privacy, and online safety.
- **Ensure compliance** with data protection laws
- **Use privacy-friendly platforms** with minimal tracking.
- **Encourage critical thinking** about targeted content and ads.
- **Provide clear opt-in/opt-out choices** for cookie use.

Further reading: **Cookies and similar technologies | ICO**

Appendix 3

Key guidelines for handling digital disclosures

1. **Stay calm and professional**
   - Maintain a calm manner, regardless of the content being shared.
   - Avoid displaying shock, judgment, or alarm, as these reactions could discourage the individual from continuing to share.
2. **Acknowledge and listen**
   - Thank the individual for trusting you enough to share their concerns and actively listen without interrupting.
   - Validate their feelings and assure them they've done the right thing by speaking up.
3. **Do not promise confidentiality**
   - Be transparent about your responsibility to share the information with relevant people or authorities if necessary for their safety.
   - Use clear language to explain what you can and cannot keep private, avoiding promises that you cannot fulfil.
4. **Follow your organisation's safeguarding policy and procedures**
   - Notify your designated safeguarding officer or an appropriate authority without delay.
   - Keep the individual informed of the steps being taken and why they are necessary.
5. **Document the disclosure**
   - Record the disclosure as soon as possible, ensuring your notes are:
     - **Accurate**: write down the exact words used by the individual without interpretation or assumptions.
     - **Factual**: avoid opinions or judgments; stick to what was shared and your actions in response.
     - **Comprehensive**: include the date, time, platform used, and details of any advice or next steps provided.
   - Store all documentation securely in line with your organisation's policies.
6. **Assess risk and respond appropriately**
   - Determine if the individual is at immediate risk of harm to themselves or others.
   - If there is an urgent danger, contact emergency services immediately.
   - Provide reassurance and explain any immediate steps you're taking to protect them.
7. **Respect privacy and data protection**
   - Only share the disclosure with authorised individuals, ensuring compliance with data protection laws such as GDPR.
   - Secure all sensitive information to prevent unauthorised access or breaches.
8. **Offer support and resources**
   - Provide the individual with information about relevant support services, such as:
     - Counselling organisations.
     - Helplines (e.g., mental health or abuse hotlines).
     - Specialist charities or local support groups.
   - Follow up, if appropriate, to ensure they feel supported and know how to access help.

Appendix 4

'Our Agreement' for Online Delivery
Below is an example agreement you can use when working with young people, which includes some specifics about online delivery. Sometimes this is called a code of conduct. You can read this alongside our checklist for youth work online.

Where possible it should be co-produced with young people at the start of any session. This will help you tailor it to the young people you are working with e.g. age-appropriate language, specific experiences etc. This will help you best meet the needs of each group of young people.

Together we, both youth workers and young people, agree to:

- **Get involved and encourage others to do the same.** We will engage with the sessions as much as possible and be encouraging of others to take part too.
- **Respect each other and listen.** We will be kind, respectful, supportive and non-judgemental of everyone. We will create a space for people to be heard and wait until it's our turn to speak. This might mean muting our mics until speaking too.
- **Think about our language, clothing, and space.** We will make sure we are appropriately dressed, decide whether to blur our background and think about the words we use.
- **Keep the session invite only**. Do not share the access link and /or password. We want to know who is attending and this will mean having a completed participation or consent forms. Also, where appropriate, at the start of any session everyone will turn their cameras on to make sure the right people are here. The session link will not be shared with anyone else.
- **Have fun and engage!** This space is for you, we hope you enjoy being here! We will be on time, stick to planned breaks and finish on time too. If things have to change, we'll let you know as soon as possible.
- **Work together and be flexible with our digital behaviours.** We will adapt the session to best suit our needs wherever possible e.g. not requiring cameras on the whole time and / or integrating the chat function to our session. We'll talk about what's working and not working.
- **Being safe:** If you are worried about something or someone, please reach out to your youth worker or trusted adult as soon as you can. If we, as the youth workers, are worried about you (sometimes called a safeguarding concern) we will tell you and only share with people who need to know. Hopefully we will do this with you knowing and maybe even with you.
- **What else is important to get the best from our online session today?**

Appendix 5

Data Protection Checklist for Signing Up to a New Digital Platform or Tool in Youth Work

Delivering safer and high-quality online youth work involves several key considerations. Here are some key questions to help you navigate your way through our tipsheet:

	Action	Notes
1	Identify the platform and rationale for its use • Have young people expressed an interest in using this platform? • Why • What do you plan to deliver in the space/place?	
2	Permissions • Has your management team approved the use of this platform? • Is your organisations Data Protection Officer aware?	
3	Data Protection Impact Assessment (DPIA) • Do you need to complete a DPIA? • Have you completed a DPIA?	
4	Privacy and Data Handling • Have you reviewed the platform's privacy policy and terms of service. • Have you checked how the platform handles data collection, storage, and sharing. • Have you ensured only necessary data is collected? • Have you verified the platform's security measures? (encryption, secure access, etc.). • Have you checked for compliance with relevant data protection regulations? (e.g., GDPR). • Have you ensured you can delete data when it is no longer needed? • Have you checked the platform's procedures for data breaches and incident response? • Have you ensured there are clear steps for reporting and handling data breaches?	
5	Consent: • Have you remembered the digital age of consent? A young person needs to be 13 or over to sign up and use most platforms. • Have you obtained consent from participants and their parents (where applicable)? • Have you ensured the consent process is clear and easily understandable?	
6	Access and User Controls: • Have you set up strong authentication methods (e.g., multi-factor authentication)? • Have you defined and managed user roles and permissions carefully, regularly reviewing them? • Have you ensured spaces are password protected and that verified young people can only access them with staff present?	
7	Training and Awareness: • Do you provide training for staff and volunteers on data protection and platform use? • Do you keep everyone informed about their responsibilities regarding data protection?	

Appendix 6

Digital Youth Work Checklist for Online Delivery

Delivering safer and high-quality online youth work involves several key considerations. Here are some key questions to help you navigate your way through our guidance:

1	Is your approach needs led?	
2	Do you have sound knowledge of online safety and wellbeing?	
3	Have you trialled and tested the platform(s)?	
4	Have you considered Data Protection and taken appropriate steps?	
5	Have you completed a risk assessment?	
6	Have you got a verification process in place?	
7	Do you have consent from parents and young people?	
8	Do young people know how to use the space and is a code of conduct in place?	
9	Is the space lockable/ password protected?	
10	Have you gone through the steps in this guidance?	