Digital Safeguarding Procedure

Unique reference number: PP-SG-PR-001

Document Owner: Chris Roach, Head of Safeguarding

Version: 1.0

1. Purpose of Procedure

The Digital Safeguarding Procedure is designed to ensure that our staff and volunteers consider all of our digital and online interactions with each other and with service users, supporters, donors and members of the public; that these are as safe as possible, and all known risks are recorded and mitigated.

2. Scope

This procedure applies to all Guide Dogs staff and volunteers, both during and outside normal working / volunteering hours. It sets out Guide Dogs' approach to digital safeguarding and covers all digital and online spaces where Guide Dogs' work is conducted. This includes but is not limited to: Email; Internal and external websites; Social Media channels and online platforms relating to Guide Dogs' work (including Facebook, Twitter, Instagram, YouTube, WhatsApp, LinkedIn, Pinterest, TikTok, Twitch and Discord, Blogs); Online training delivery (via Zoom and Teams); Websites (including those relating to fundraising and e-commerce); Internet Services and IS equipment provided by Guide Dogs.

3. Definitions and Key terms

- The Digital Manager is the person responsible for the service or platform, for example a Facebook page or a gaming platform, they are responsible for ensuring the correct checks and balances in place to maintain a safe environment. This will ensure that anyone who has access to that platform is clear about their role and

responsibilities, and that any guidance, training or risk assessments are in place before anyone has access to that area.

- Online means, activity where someone or something currently is connected to the Internet.
- Digital, means a format or a process that describes electronic technology that generates, stores, and processes data.
- Digital safeguarding refers to the policies, procedures and practices relating to digital and online spaces and how we interact with others in a safe way regarding risk, including content, contact and conduct. The same safeguarding principles apply to Guide Dogs' activities, whether these take place digitally or in-person. The terms Digital and online activity will be used interchangeably throughout this document.

There are specific considerations to take into account with online initiatives, as digital technology has brought about new safeguarding issues. For example, perpetrators of exploitation, abuse and harassment can hide behind fake photos and profiles, and the online disinhibition effect leads to the rise of trolling and cyberbullying (see Appendix 1 for types of online harms and definitions). Images, videos, and texts can be sent easily to large groups of people, and once images or data have been shared digitally, it is almost impossible to delete or recall them. Digital safeguarding simply means taking the necessary steps to stay safe online.

The following risks should be taken into account when considering digital safeguarding, these fall into three categories: Content Risk, Contact Risk and Conduct Risk:

Content Risk - Risks that are produced as a result of the material that people can access online. People may be exposed to this content actively or passively, and it may produce a harmful effect. Content may be illegal to possess or share e.g., sexually exploitative images of children or radicalising videos. Inappropriate and offensive content is more subjective and includes political information; commercial adverts or spam; violent, extremist, or hateful material; sexually exploitative or sexual material; and content which is discriminatory based on

someone's race, ethnicity, nationality, class, socioeconomic status, age, sex and gender identity, sexual orientation, disability, religion, language or other status.

Contact Risk - Risks that are produced as a result of others' online behaviour when the digital and physical worlds are drawn together. Individuals may have information about them shared or may be engaged in ways which lead to harmful consequences. The types of behaviour which people may experience include:

- Non-contact sexual abuse and exploitation – including grooming, flashing, being persuaded to perform sexual acts online, and being exposed to sexually exploitative images or videos.
- Distribution of private and sexual images, e.g., the distribution of sexually exploitative images or videos without an individual's permission.
- Harvesting, tracking and illegal sharing and possession of information – including having personal data collected, processed, or shared without the individual's consent or on another unlawful basis.
- Increased exposure to cybersecurity risks, e.g., by having malicious content shared such as ransomware, apps or other active content or malicious code.
- Bullying and trolling which could lead to physical contact, threats, or violence.
- Friend requests or private/direct messaging.

Conduct Risk - Risks that are produced as a result of people's own online behaviour, which may put themselves and others at risk. People may download something illegally, bully, harass or exploit others, unintentionally reveal their location, create, and upload sexual material or sext (send someone sexually explicit photographs or messages via mobile phone). This may also include online activism or breaking confidentiality of closed spaces by reposting, sharing, downloading or in other ways transmitting information that leads to harassment, exploitation, or other harm in another setting.

Digital safeguarding means protecting everyone at Guide Dogs from online harms (See Appendix 1 – Types of online harms).

4. Roles and responsibilities

Safeguarding is everybody's responsibility in Guide Dogs. We all have an important part to play in ensuring the digital safeguarding of staff, volunteers, service users, supporters, donors, and members of the public. This could include the design of new staff and volunteer roles within the digital space, online service delivery to service users, technology training by Habilitation Specialists and Vision Rehabilitations Specialists, creating digital content and responding to social media posts etc. We all need to understand the importance of using the Risk Assessment process to mitigate known or potential risks when online. Also, if we have concerns about online harms, knowing how to raise a safeguarding concern via the online reporting form, details of how to do this are contained within Section 12: Reporting a Safeguarding Concern of this document.

5. Use of equipment, internet, and social media

At Guide Dogs we use a wide range of Information Services and Technology. The Acceptable Use of Information Services and Technology Policy sets out the principles for all users of Guide Dogs' IT systems and equipment to ensure compliance with good practice and statutory requirements.

Guide Dogs uses a number of social media channels, its use, guidelines and escalation procedures when issues arise are covered in the following key documents: Social Media Policy, Social Media Procedure and Volunteer Social Media Policy.

6. Privacy, data protection and informed consent

The Data Protection Policy together with the documents and other policies referred to within it regulates and details the way in which Guide Dogs obtains, uses, holds, transfers and processes Personal Data and Special Category Data about individuals and ensures that all

employees know the rules for protecting Personal Data. The Data Protection policy also outlines individuals' rights in relation to their Personal Data being processed by Guide Dogs.

Considerations should be made for the following situations: Seeking the appropriate levels of consent, and the understanding of the context, when thinking about digital content creation relating to staff, volunteers, service users, supporters, donors, and members of the public. With regards to children, consent is from their parent or guardian. The digital creator should exercise judgement and creative skills to tell a powerful story in a way that doesn't reveal the identity of a child, young person, vulnerable adult, or someone who may be put at risk due to e.g., political or religious contexts. Digital content should not place people at risk, Guide Dogs needs to be alert to, and sensitive to, sharing content online as there may be additional risk, and this may be ongoing, such as emergency situations, Conflict situations, Abuse, Crime, this would be indicated via a safeguarding reference number displayed on Guide Dogs' databases. Content should receive the appropriate levels of sign-off when gathering content and before sharing it online and they have the right to remove any pictures or stories about them from online spaces.

7. Digital Risk Assessment and Risk management

The Digital Risk Assessment process is the same as any other risk assessment process that Guide Dogs would be conducting for in-person activity. The Digital Risk Assessment must be completed by the Digital Manager and should not be a one-off event, it should continue alongside the service design process for new services or new online interactions, it should continue to run continuously when service or activity happens once it has been launched and is considered live. The Digital Risk Assessment will influence other factors such as the continuous reviewing of this and other policies across Guide Dogs, it will support the evolution to allow and understand new online risks, add these and support further mitigating factors and actions. This way the risk assessment will be live, feeding into the wider Risk Register for the organisation. (See Appendix 2 – Risk Assessment Process)

8. Children, Young People and Adults at risk

Guide Dogs recognises that children, young people, and adults at risk, are groups who may experience specific or enhanced risk within the digital and online spaces. In these circumstances, Guide Dogs will take special measures to ensure our activities are not harmful in and of themselves, and that these groups are protected from abuse, harm, and exploitation when they engage with the organisation.

9. Breaches of the procedure

Any known breaches to this Procedure will not be accepted and may result in appropriate disciplinary proceedings for staff and relevant conduct procedure for volunteers. Guide Dogs also has in place Safeguarding Codes of Conduct for children and adults (see Knowledge Hub or VIP) linked to interactions with Service Users, supporters, donors, and members of the public.

10. Online Safety and Support

Online Safety and support

On the Guide Dogs' website we have a range of resources for children and young people to help stay safe online. We also have information about how technology can help adults, but how to keep safe online too.

Support organisations

There are a wide range of support organisations who work within the area of online safety for all, these include:

- UK Safer Internet Centre
- CEOP – Thinkuknow
- CEOP – Safety Centre
- NSPCC – Online Safety
- Childnet
- Internet Matters
- Internet Watch Foundation
- Family Online Safety Institute

Training

At Guide Dogs we have a number of learning modules available on the Learning Gateway, these include:
Cyber Security – Top Tips
Safeguarding & CYP - Online Safety for Professionals working with CYP
The Fundamentals of Cyber Security with West Midlands Police
Externally, other courses are available using this link: https://saferinternet.org.uk/events

11. Raising a concern

Anyone can raise a concern about inappropriate or worrying activity which has occurred at Guide Dogs, whether posted online or in a digital space. This could include posts on social media, responding to posts on social media, the sharing of personal information or online stalking within digital/online operated spaces etc. Initial concerns should be raised with digital managers responsible for the digital platform as appropriate; content will be monitored, and following reports will be moderated and removed.

Guide Dogs staff and volunteers have a responsibility to report any suspicions or concerns concerning digital safeguarding and the issues outlined in this Procedure. Anyone can raise a concern to Guide Dogs' Safeguarding Team about an incident they have experienced, witnessed, or heard about concerning Guide Dogs' online activity that could relate to abuse, harm, well-being, or personal safety etc.

Guide Dogs' Safeguarding Children and Young People's Procedure and Safeguarding Adults Procedure apply, when a safeguarding concern is raised relating to digital and online activity. It is vital that we use the 4 Rs of safeguarding: Recognise, Report, Record and Respond. It is important to report a safeguarding concern or call the Safeguarding Team for advice and support.

12. Responding to a concern

It is important that appropriate action is taken quickly and sensitively when concerns are raised, this will include digital managers ensuring

content is monitored, moderated, and removed. When a safeguarding referral is made, key actions will be made by the Safeguarding Team, which may include making links with other key functions including HR, Volunteering, IS, Operations etc as and when required. All relevant Safeguarding procedures and relevant actions will be undertaken to safeguard the staff member, volunteer, service user, donor, supporter or member of the public.

Appendix 1 - Types of online harms and definitions

Digital safeguarding means protecting everyone at Guide Dogs from online harms including, but not limited to:

- Creeping – Persistently checking up on someone on social media. Creepers hide from you by not inviting, commenting, or responding on Facebook and other social media platforms.
- Cyberstalking – Repeatedly using electronic communications to harass or frighten someone. For example, by sending threatening messages.
- Doxing or Identity Theft – Takes place when someone gets hold of personal information about you – such as your real name, address, job, other personally identifiable data and posts it on the internet without your consent.
- Discrimination - Abuse on the grounds of protected characteristics – It can be an offence to stir up hatred – 'inciting hatred' - on the grounds of any of the protected characteristics.
- Disinformation - Deliberate intent to spread incorrect information.
- Hacking – Accessing or using computer systems or networks without authorisation, often by exploiting weaknesses in security.
- Harmful online challenges – Online challenges sometimes show people doing dangerous things. People share these posts on social media, encouraging others to do the same.
- Hoaxes – A lie designed to seem truthful.
- Impersonation or ‘catfishing’ - Where someone pretends to be someone else online. This is often by taking photos from social media to build a fake profile.
- Misinformation - Where someone shares information, they think is correct, but it isn’t.
- Cyberbullying /Online bullying - Offensive, intimidating, malicious, insulting behaviour and abuse of power online. This can humiliate or denigrate people.
- Online harassment - Unwanted contact online intended to violate someone’s dignity. It could be hostile, degrading, humiliating or offensive.

- Online Scams – Scams are happening increasingly through the internet and email. You are more likely to fall victim to fraud or cyber offences above any other crime. These could include phishing emails, fake websites and other ways to get your money.
- Promotion of self-harm, suicide and eating disorders – Content encouraging these harmful behaviours on social media.
- Promotion of violent behaviour - Recording of an assault for the purpose of widely sharing the recording.
- Radicalisation - Radicalisation aims to inspire new recruits, embed extreme views and persuade vulnerable people to support a cause. This may be through a direct relationship, or through online gaming and social media.
- Sexual exploitation and grooming online - Developing a relationship with a child with the intention of abusing them. Offenders use emotional and psychological tricks to build relationships. The abuse can take place online or offline.
- Sharing of illegal and inappropriate imagery - 'Illegal' means child sexual abuse imagery and imagery that incites violence, hate or terrorism. 'Inappropriate' could mean sharing pornography, or violent or hateful content.
- Trolling – Intentionally upsetting, shocking or winding up selected individuals or groups of people.
- Oversharing personal information - This includes information that makes someone identifiable, like their name or phone number. It may also include identifying details based on someone's protected characteristics.

Appendix 2 - Risk Assessment Process

Researching the risks

Using the risk assessment tool to list all of the possible risks associated with that digital activity or space. 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.

Here are some examples of risks from various online delivery and interactions:

Video-based services

- Call quality is poor, or call disconnects user becomes confused and unsettled and staff fail to hear important things they are saying.
- Inadequate security settings: leave conversations vulnerable to being hacked or traced.
- Being witnessed leads to further harm: a user (or users) who is at risk of abuse or harm is overheard/seen contacting others in such a way as to increase harm and risk to that individual.
- User discomfort at being visible: users with poor mental health or experiencing trauma or body dysmorphia may feel uncomfortable being visible. This is more likely when the user and worker have not previously met or established trust.
- Overwhelmed by group work in an unfamiliar setting: the nature of video calling where delays might occur, social cues are different and individuals risk speaking over one another leaves individuals feeling distressed and upset.

- User discloses abuse in a group setting: member makes a disclosure witnessed by others.

Messaging based services

- Messages read by others leads to further harm: a perpetrator finds out a victim is reaching out for support and inflicts further harm.
- Third party impersonates user: lack of visual or vocal cues in messaging allows third party to reply to service messages, leading to misinformation.
- Worker or user misunderstands message: leading to distress, confusion or harm.
- Inappropriate communications: messaging that can lead to inappropriate levels of contact of a personal nature, over familiarisation and possible grooming.

Live chat and chatbot services

- Being witnessed or overheard leads to further harm: a user (or users) who is at risk of abuse or harm is overheard/seen contacting others in such a way as to increase harm and risk to that individual.
- User receives bad information: chatbots or call handlers give inappropriate or incorrect information because they haven't been updated.
- Chatbot fails to identify safeguarding issue: because they were not kept up to date or safeguarding journeys weren't designed in.
- Communication style distresses user: inappropriate online communication styles from chatbots or staff upsets users

Online groups and forums

- User overshares personal information: member shares personal information in a way that compromises their security or privacy.
- User discloses abuse: member discloses to the group.
- User shares triggering content: member shares content that distresses rather than supports other members.
- Inappropriate behaviour towards other members: this may include discussing inappropriate topics, using offensive language or bullying others, causing upset and distress.

- Anonymity leading to ineffective safeguarding: forums that allow users to create an avatar or pseudonym limit a service's ability to provide support or escalate risk. Anonymity may also provide an opportunity for impersonation.
- Fake profiles aka 'catfishing': perpetrators impersonate others or use a false profile to gain access to a private group.
- Grooming and inappropriate contact: unrestricted access allows for inappropriate contact from potential perpetrators of harm. Particularly relevant when running groups or creating interactive games for children and young people.

Content

- Content or images upset user: users become upset and/or triggered after viewing inappropriate images, words, videos or sound clips.
- User misled by information: information causes harm because it is incorrect, misleading, outdated or inappropriate.
- User is witnessed viewing content: perpetrator witnesses user reading content or views their browsing history, increasing risk of harm.
- User-generated content puts them at risk: content isn't properly anonymised or includes sensitive or legal information.

Data and devices

- User receives breached device: putting a service user's privacy and security at risk.
- Existing risk of abuse is increased: user experiencing offline abuse becomes at risk of online abuse from an existing perpetrator.
- User fails to maintain device security or take precautions make them vulnerable to privacy breaches, scams and abuse.
- User uses device in a way that creates risk: poor awareness of how to communicate and handle information online puts the user at risk of harm from others or harm to themselves through oversharing or inappropriate behaviour.

Assessing the risk

Using the information gathered to populate the Risk Assessment tool looking at:

- Risk (description of something going wrong)
- Impact (rating 1-5)
- Likelihood (rating 1-5)
- Risk rating (Impact x Likelihood)
- Existing control measures (mitigation activities already being done)
- Control measures (mitigation activities you will do)
- Who is responsible?
- Accepted? (whether the risk, with its control measures in place, has been accepted by your organisation)
- Actioned (date you implemented mitigations)
- Review date

Make decisions and documenting them.

The Safeguarding Risk Assessment Matrix will support with decision making and help the organisation understand the steps needed to mitigate risks and the tools to support delivery and online interactions, noting key points and rationale for the chosen method of delivery or interaction. As these decisions are recorded and assessed by a group of people it takes emphasis away from one decision maker and a consensus approach for safe digital services and interacting online.

Review process

Reviewing risks should happen regularly based upon the launch of the service or activity. When a service or activity is new, this should occur more often during this phase. When it is more established this should be set within a regular timeframe and revisiting this process if elements of services or online activity change or alter.

Measures:

Procedure Instructions

See points 11 and 12 above.

Documentation:

Safeguarding Risk Assessment Matrix Template

Permissible exceptions:

None

Related Policies or Processes:

Acceptable Use of Information Services and Technology Policy - BF-IS-P-012

Data Security Procedure - BF-IS-PR-009

Information Security Policy - BF-IS-P-013

Key Safeguarding Principles – PP-SG-S-001

Safeguarding Adults - Code of Conduct for Staff and Volunteers - PP-SG-S-004

Safeguarding Adults Procedure - PP-SG-PR-004 (PROHR35)

Safeguarding Children and Young People's Procedure – PP-SG-PR-003 (PROHR34)

Safeguarding Children – Codes of Conduct for Staff and Volunteers – PP-SG-S-003

Safeguarding Prevent Policy – PP-SG-P-001

Social Media Policy - PP-HR-P-056

Social Media Procedure - PP-HR-PR-056

Volunteer Social Media Policy – PP-VOL-P-001

Governance Information. Please do not remove.

Governance Review & Approval Table*:

The table below contains two rows and five columns.

Governance Area:	H&S	Protection of Children & Adults	Insurance	Legal	GDPR
Date Approved:		06/07/23			

Review Frequency:

Procedures - Core: Annually

Procedures – Subject Specific: Every 2 years

Reviews should be done in accordance with relevant regulation, legislation changes or as a result of ad hoc activity, such as continuous improvement initiatives.

Version control table:

The table below contains four rows and four columns. (Only the original approval date and the most recent amendment should be included in the table.)

Date	Version	Status	Details of Change
:	1.0	Approved	:

***Please see below when a document must be reviewed by Governance**

Safeguarding - All documents with any reference to safeguarding, recruitment and training, working with clients (Adult and CYP).

Legal - All documents with any reference to agreements or contracts, third party partnerships, potential reputational risk, reference to compliance with any statutory or regulatory obligation.

Health and Safety - All documents where an activity could cause harm to a member of staff, service user, volunteer or third party or where there is reputational risk.

Insurance – A change to the way we deliver our services.

GDPR – If we are gathering any personal information on volunteers or service users.

End of document