



ARK OF HOPE FOUNDATION FOR ALL NATIONS

Digital Safeguarding Policy

Protecting children, young people and adults at risk in every digital space we operate — communication, remote service delivery, social media and data.

Registered Charity No. **1161228**

Version **1.2**

Review Date **18 August 2027**

Ark of Hope Foundation For All Nations

PO Box 4954, Stoke-on-Trent, ST4 9RW
info@arkofhopefoundation.com | 01782 899084

Policy Owner: **Designated Safeguarding Lead**

Approved By: **Board of Trustees**



Contents.

A full index of policy sections and supporting appendices.

1	Policy Statement and Core Principles
2	Scope and Application
3	Legal and Regulatory Framework
4	Definitions and Key Terminology
5	Roles and Responsibilities
6	Digital Safeguarding Risk Assessment
7	Safe Use of Digital Platforms and Communication
8	Social Media Policy and Procedures
9	Remote Service Delivery – Detailed Procedures
10	Use of Personal Devices and Bring Your Own Device (BYOD)
11	Photography, Video and Image Sharing
12	Data Protection, Privacy and Information Sharing
13	Online Safety Act 2023 – Compliance and Duties
14	Working Together to Safeguard Children 2026 – Implications
15	Reporting and Responding to Concerns – Detailed Procedure
16	Recording and Record-Keeping
17	Allegations Against Staff or Volunteers
18	Training and Awareness
19	Monitoring, Evaluation and Review
20	Related Policies and Documents
21	Approval and Sign-off

Appendices

A	Safeguarding Report Template
B	Incident or Cause for Concern Report Template
C	Contact Details for Safeguarding Reporting
D	ICE (In Case of Emergency) Card
E	Guidance on Mental Capacity



F **Body Map**

G **Flowchart for Responding to a Child Safeguarding Concern**



1

Policy Statement and Core Principles

1.1 Statement of Intent

Ark of Hope Foundation For All Nations takes its responsibilities to all its service users, staff, volunteers, and community members seriously. We recognise a particular responsibility to children, young people, and adults at risk of abuse or neglect, and we understand that our commitment to supporting vulnerable populations means many of those we work with may be at risk.

We recognise that digital technologies, including the internet, social media, mobile devices, video conferencing, messaging applications and online platforms, are integral to how we deliver services, communicate with beneficiaries, and operate as an organisation.

We also recognise that digital environments present specific and often heightened safeguarding risks. These include, but are not limited to:

- Online grooming, exploitation and abuse
- Cyberbullying and harassment
- Exposure to inappropriate, harmful or illegal content
- Privacy breaches and data security incidents
- Unauthorised sharing of images or personal information
- Identity theft and impersonation
- Coercive control and domestic abuse facilitated through digital means
- Radicalisation and exposure to extremist content
- Financial exploitation through online scams and fraud

This Digital Safeguarding Policy sets out our comprehensive commitment to ensuring that all digital activity undertaken by Ark of Hope Foundation For All Nations, its staff, volunteers, trustees and beneficiaries is conducted safely, responsibly and in accordance with our broader safeguarding framework and all relevant legislation.

This policy is based on national guidance on Safeguarding Adults and Safeguarding Children, including standards set by CCPAS and the Staffordshire and Stoke-on-Trent Adult Safeguarding Partnership Board and Stoke-on-Trent Safeguarding Children Partnership (SSCP).

This policy is to be adhered to by all Ark of Hope Foundation For All Nations staff and volunteers.

1.2 Core Principles

Our digital safeguarding approach is guided by the following core principles, which align with our organisational values:

- Protection without exception – Every child, young person, woman, beneficiary, volunteer and partner is protected from harm, abuse and exploitation in digital contexts, regardless of age, gender, disability, religion, ethnicity, nationality, immigration status or any other characteristic.



- A safeguarding culture – We will foster a culture where digital safeguarding is prioritised, where concerns can be raised openly, and where everyone feels confident to speak up without fear of reprisal.
- Prevention through proactive measures – We will take proactive steps to prevent digital harm, abuse and exploitation through clear policies, robust recruitment, ongoing training, and regular risk assessments.
- Proportionate and timely response – We will respond swiftly, appropriately and proportionately to all digital safeguarding concerns and allegations.
- Continuous improvement – We will regularly review and update our digital safeguarding policies and procedures, at least annually, in response to emerging risks, new technologies, and changes in legislation.
- Partnership and collaboration – We will work in partnership with statutory agencies, local safeguarding partnerships, and other organisations to ensure the best outcomes for those at risk.
- Empowerment and ‘Making Safeguarding Personal’ – We will adopt a person-centred approach to digital safeguarding, where the individual must be involved in always making decisions about their own safety, balancing acceptable risk with the duty to protect. This aligns with our organisational ethos of empowerment and having service user-led goals and personal development plans.

2 Scope and Application

2.1 Who This Policy Applies To

This policy applies to:

- All Trustees of Ark of Hope Foundation For All Nations
- All staff, whether paid or voluntary, including full-time, part-time, temporary and fixed-term
- All volunteers and interns, regardless of the duration or nature of their role
- All contractors, consultants and partners delivering services on our behalf
- All beneficiaries, including children, young people and adults at risk, who engage with our digital services or platforms

Safeguarding is the responsibility of everyone connected with our organisation. All those covered by this policy are expected to read, understand and follow this guidance.

2.2 What This Policy Covers

This policy covers all digital activity undertaken by or on behalf of Ark of Hope Foundation For All Nations, including but not limited to:

A. Communication with Beneficiaries

- Video calls and virtual meetings (Zoom, Teams, WhatsApp video, etc.)
- Voice calls and voice messages



- Email communication
- SMS and text messaging
- Messaging applications (WhatsApp, Signal, Telegram, etc.)
- Social media direct messaging (Facebook Messenger, Instagram DMs, X/Twitter DMs, etc.)
- Online forums and discussion groups

B. Remote Service Delivery

- Virtual support sessions and counselling
- Online group activities and workshops
- Digital casework and advocacy
- Virtual drop-in sessions
- Online mentoring and befriending

C. Social Media

- Organisation accounts (Facebook, Instagram, X/Twitter, LinkedIn, TikTok, etc.)
- Content creation and sharing
- Comment moderation and engagement
- Live streaming and video content
- Paid advertising and promotional activity

D. Websites and Online Platforms

- Organisation website
- Online portals and digital platforms used for service delivery
- Booking and registration systems
- Donation platforms

E. Data and Information

- Storage and sharing of beneficiary data
- Cloud-based document storage (Google Drive, OneDrive, Dropbox, etc.)
- Use of databases and CRM systems
- File transfer and sharing

F. Personal and Staff Digital Activity

- Use of personal devices for work purposes (BYOD)
- Personal social media use in a professional context
- Remote working and home-working digital security
- Use of organisation devices for personal purposes



3

Legal and Regulatory Framework

This policy is informed by and complies with the following legislation, statutory guidance and regulatory requirements:

3.1 Primary Legislation and Statutory Guidance

Legislation / Guidance	Key Provisions
Working Together to Safeguard Children 2026	Statutory guidance on multi-agency working to help, support and protect children in England. Applies to voluntary, charity, social enterprise and faith-based organisations with functions relating to children.
Online Safety Act 2023	Creates duties for providers of regulated user-to-user services, search services and services that publish or display provider pornographic content. Ark of Hope will assess whether any online service it operates falls within scope before treating the Act as directly applicable.
UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018	Governs the processing, storage and sharing of personal data. Requires lawful basis for processing, data minimisation, security measures, and subject access rights.
Safeguarding Vulnerable Groups Act 2006	Provides the legislative framework for vetting and barring of individuals working with children and vulnerable adults.
The Care Act 2014	Sets out the statutory framework for adult safeguarding, including the duty to promote individual wellbeing and protect adults at risk from abuse and neglect. Our definition of an 'adult at risk' follows the Care Act 2014.
Protection of Freedoms Act 2012	Established the Disclosure and Barring Service (DBS) and the barred lists.
Counter-Terrorism and Security Act 2015	Places a duty on specified authorities to have due regard to the need to prevent people from being drawn into terrorism (Prevent duty).
Domestic Abuse Act 2021	Recognises domestic abuse as a broader pattern of controlling, coercive or threatening behaviour, including digital and online abuse.
Equality Act 2010	Protects individuals from discrimination, including on the basis of protected characteristics in digital and service contexts.
Children Act 1989 and Children Act 2004	Sets out core duties relating to children in need, child protection enquiries and safeguarding arrangements, including the definition of a child as a person under the age of 18.
Care and Support Statutory Guidance under the Care Act 2014	Provides statutory guidance on adult safeguarding, including section 42 enquiries, safeguarding adults boards, person-centred practice and Making Safeguarding Personal.



3.2 Regulatory and Sector Guidance

Guidance	Key Provisions
Charity Commission guidance on social media (updated April 2026)	Updated to incorporate the Online Safety Act 2023. Sets out that charities must reflect in their social media policy how they will comply with the Act.
Charity Commission guidance: Safeguarding and protecting people for charities (2025)	Sets out trustees' legal duties to safeguard and protect beneficiaries, including in digital contexts.
Charity Digital Code of Practice (2025)	Provides guidance on digital leadership, data-driven approach, and keeping people safe online.
Data (Use and Access) Act 2025	Updates data protection framework, including provisions on data sharing for safeguarding purposes.
Ofcom guidance on the Online Safety Act	Provides practical guidance on risk assessments, illegal content, and children's safety duties.
Information Sharing: Advice for practitioners providing safeguarding services to children, young people, parents and carers (2018)	Provides guidance on effective information sharing for safeguarding purposes.
Action on Elder Abuse	Defines abuse as "a single or repeated act occurring within a relationship where there is an expectation of trust which causes harm to an individual."

4

Definitions and Key Terminology

4.1 Safeguarding

Safeguarding means protecting people's health, wellbeing and human rights, and enabling them to live free from harm, abuse and neglect. It is the responsibility of all organisations and individuals working with children and adults at risk.

4.2 Children and Young People

For the purposes of this policy, a child or young person is anyone under the age of 18, in line with the Children's Act 1989 and UK legislation.

4.3 Adults at Risk

An adult at risk is any person aged 18 or over who (following the Care Act 2014):

- Has needs for care and support (whether or not the authority is meeting any of those needs)
- Is experiencing, or is at risk of, abuse or neglect
- As a result of those needs, is unable to protect himself or herself against the abuse or neglect or the risk of it



Our beneficiaries include women and families facing poverty, homelessness, domestic abuse, insecure immigration status, and multiple disadvantage. Many of the adults we support are therefore considered adults at risk.

4.4 Digital Safeguarding

Digital safeguarding refers to the measures, policies and procedures put in place to protect children and adults at risk from harm, abuse and exploitation arising from or facilitated through digital technologies and online environments.

4.5 Types of Digital Abuse and Harm

Type of Harm	Description and Examples
Online Grooming	An adult builds an emotional connection with a child or young person online to gain trust for the purposes of sexual abuse, exploitation or trafficking.
Cyberbullying	Repeated, deliberate harassment, intimidation or humiliation using digital technologies, including social media, messaging apps and online forums.
Digital Domestic Abuse	Use of technology to control, monitor, coerce or threaten a partner or family member, including tracking apps, social media surveillance, and controlling access to devices.
Image-Based Abuse	Non-consensual sharing of intimate images, including “revenge porn” and “deepfake” images.
Online Exploitation	Using digital platforms to exploit individuals, including for sexual purposes, forced labour, or criminal activity.
Exposure to Inappropriate Content	Accessing or being exposed to harmful, illegal or age-inappropriate content online.
Sexting and Youth-Produced Sexual Imagery	Sharing of sexual images or videos by young people, including consensual and non-consensual sharing.
Online Radicalisation	Exposure to extremist or terrorist content designed to radicalise individuals.
Digital Financial Abuse	Using digital means to control or exploit an individual’s finances, including online scams and fraud.
Identity Theft and Impersonation	Using another person’s identity or creating fake profiles to cause harm.
Trolling	Posting inflammatory, offensive or provocative comments online to upset or provoke a response.
Doxxing	Publishing private or identifying information about an individual online without consent, often to harass or threaten them.
Child Sexual Exploitation (CSE) Online	Coercing or manipulating a child into sexual activity in exchange for something they need or want, occurring via digital platforms.



Type of Harm	Description and Examples
Modern Slavery (Digital Facilitation)	Using digital means to control, coerce or exploit individuals, including holding documentation electronically or using digital surveillance.

4.6 What Constitutes Abuse?

Abuse may consist of a single act or repeated acts, but is rarely accidental. It may be physical, verbal, or psychological; it may be an act of neglect or an omission to act. Abuse can occur when a vulnerable person is persuaded to enter into a financial or sexual transaction to which they have not consented or cannot consent. It varies from trafficking workforces across the globe to domestic violence within a home.

4.7 Safeguarding is Everyone's Responsibility

Employees and volunteers have a responsibility to be aware of and alert to signs that all is not well with a service user, volunteer, or staff member. However, they are not responsible for diagnosing, investigating, or providing a therapeutic response to abuse. Not all concerns relate to abuse; there may well be other explanations.

5 Roles and Responsibilities

5.1 Board of Trustees

The Board of Trustees has ultimate responsibility for digital safeguarding within Ark of Hope Foundation For All Nations. Trustees are responsible for:

- Approving this Digital Safeguarding Policy and any subsequent updates
- Ensuring the policy is reviewed at least annually
- Ensuring the policy is effectively implemented and monitored
- Ensuring compliance with Charity Commission regulations, including the requirement to report serious incidents
- Ensuring adequate resources are allocated to digital safeguarding, including training and technology
- Receiving and considering regular safeguarding reports from the Designated Safeguarding Lead

5.2 Designated Safeguarding Lead (DSL) – Child Safeguarding Lead

The Designated Safeguarding Lead (also referred to as the Child Safeguarding Lead) is the primary point of contact for all safeguarding concerns, including digital safeguarding concerns. Responsibilities include:

- Receiving, assessing and recording all safeguarding concerns
- Ensuring appropriate action is taken, including referral to external agencies
- Providing advice and support to staff and volunteers on safeguarding matters



- Liaising with external agencies (e.g., Stoke-on-Trent Safeguarding Children Partnership, Staffordshire Police, LADO, Adult Social Care)
- Ensuring secure and accurate safeguarding records are maintained
- Reporting regularly to the Board of Trustees
- Leading on digital safeguarding risk assessments and reviews
- Ensuring staff and volunteers receive appropriate digital safeguarding training
- Ensuring that the organisation's safeguarding policies and procedures are fit for purpose

Designated Safeguarding Lead / Child Safeguarding Lead

Stella King, Project Lead
Mobile: 07956120599
Email: info@arkofhopefoundation.com

Deputy Safeguarding Lead

Deborah Newbould

5.3 All Staff and Volunteers

Every member of staff and volunteer is expected to:

- Read and understand this Digital Safeguarding Policy
- Complete digital safeguarding training appropriate to their role
- Be alert to signs of digital harm, abuse and exploitation
- Report any digital safeguarding concerns promptly to the Designated Safeguarding Lead
- Follow the reporting procedures set out in this policy
- Maintain appropriate professional boundaries with beneficiaries in all digital interactions
- Treat all beneficiaries with dignity and respect in digital contexts
- Use only organisation-approved platforms and devices for work-related digital communication
- Not use personal social media accounts to communicate with beneficiaries
- Not share personal contact details with beneficiaries
- Gather information and report concerns, not decide whether abuse has occurred
- Record any incidents or concerns promptly

5.4 Managers' Responsibilities

Managers at Ark of Hope Foundation For All Nations have additional responsibilities in relation to digital safeguarding. They are responsible for:

- Supporting staff to identify digital safeguarding concerns
- Providing additional oversight of ongoing digital safeguarding concerns
- Supporting the Safeguarding Lead with multi-agency work related to safeguarding
- Appropriately supporting and supervising staff
- Supporting teams to reflect on best practices and identify areas for improvement
- Identifying gaps in knowledge, arranging training, and maintaining training logs
- Adhering to safer recruitment policies



- Maintaining the safeguarding log accurately and in a timely manner

Managers are not trained to make decisions about how best to manage safeguarding situations independently. Actions must arise from consultation with the Safeguarding Lead.

5.5 Notification and Reporting to the Safeguarding Lead

In the event of the following safeguarding concerns, the Safeguarding Lead must be informed, and a written report must be emailed within 24 hours using the Ark of Hope safeguarding template:

- Sexual offence by a tenant or ex-tenant, including an allegation
- Sexual offence where a tenant is the victim
- Significant violence by a tenant or ex-tenant
- Arson by a tenant or ex-tenant
- Child protection, where the child is a victim of a sex offence or at risk of harm by a tenant (including their parent)
- Threats of violence or harm towards a member of staff, volunteer, or member of the public (such as a neighbour)
- Any digital safeguarding incident involving the above categories

The above categories of concern will be passed to the Founder and Project Lead, Chairperson, and designated safeguarding Trustees of Ark of Hope Foundation For All Nations.

6

Digital Safeguarding Risk Assessment

6.1 Purpose and Frequency

Ark of Hope Foundation For All Nations will conduct and maintain a comprehensive digital safeguarding risk assessment to identify, evaluate and mitigate risks associated with our digital activities. The risk assessment will be:

- Reviewed annually as a minimum
- Reviewed whenever there is a significant change in our digital activities, services or platforms
- Reviewed following any safeguarding incident or near miss
- Reviewed in response to any new legislation, guidance or regulatory requirement

6.2 Areas of Risk Assessment

Risk Area	What We Will Assess
Illegal Content Risks	The risk that beneficiaries or staff encounter illegal content through our digital platforms or communications (in line with Online Safety Act 2023 requirements).



Risk Area	What We Will Assess
Children's Access Risks	The specific risks to children and young people engaging with our digital services, including access to inappropriate content and contact with potential abusers.
Behavioural Risks	The risk of harmful behaviour between users, including cyberbullying, grooming, exploitation, and harassment.
Technical Risks	Risks relating to data breaches, unauthorised access, platform security, and technical failures.
Staff and Volunteer Risks	Risks arising from staff/volunteer conduct online, including inappropriate communication with beneficiaries, boundary violations, and personal social media use.
Racism and Discrimination Risks	Risks arising from discriminatory content or behaviour online, in line with Working Together 2026's strengthened expectations for anti-racist and anti-discriminatory practice.
Multiple Harms Risks	The risk that beneficiaries may experience multiple harms simultaneously, including online harms and group-based exploitation.
Privacy and Data Protection Risks	Risks relating to the processing, storage and sharing of personal data in digital contexts.

6.3 Risk Assessment Process

- Identify – identify all digital activities, platforms and services used by Ark of Hope Foundation For All Nations
- Assess – assess the risks associated with each, considering likelihood and impact
- Evaluate – evaluate the overall risk level and prioritise for action
- Mitigate – identify and implement mitigation measures
- Monitor – monitor the effectiveness of mitigation measures
- Review – review and update the risk assessment regularly

6.4 Risk Reduction Plans (RRP)

Deteriorating mental health or the emergence of previously undisclosed mental health concerns may render an individual too high-risk for our level of support, necessitating reconsideration of their suitability for Ark of Hope accommodation. The Risk Reduction Plan must be reviewed for all residents, and any digital safeguarding risks should be incorporated into these plans.



7

Safe Use of Digital Platforms and Communication

7.1 Approved Platforms and Channels

Staff and volunteers must only use approved platforms for communication with beneficiaries. Use of unapproved platforms requires prior authorisation from the Designated Safeguarding Lead.

Purpose	Approved Platforms	Notes
Video Calls	Zoom, Microsoft Teams, Google Meet	Must use organisation account, password-protected, waiting room enabled
Voice Calls	Organisation mobile phone, landline	Do not use personal mobile numbers
Email	Organisation email address (@arkofhopefoundation.com)	Do not use personal email addresses
Messaging	WhatsApp (organisation account), Signal	End-to-end encryption required
Social Media Messaging	Facebook Messenger, Instagram DMs	Respond via organisation account only, move to secure channel for sensitive information

7.2 General Communication Standards

- Professional tone – all communication must be professional, respectful and appropriate
- Transparency – communication should be clear about who is communicating and the purpose of the communication
- Record-keeping – significant communications should be recorded in the beneficiary's case file (field notes)
- Boundaries – maintain appropriate professional boundaries; do not share personal information or engage in social relationships
- Consent – obtain consent for communication methods where required
- Reporting – report any concerning communication immediately to the DSL

7.3 Video Call Safeguarding Procedures

Before the call:

- Use an organisation-approved video platform
- Set a password and use waiting room/meeting lobby
- Ensure the meeting link is not shared publicly
- Confirm the beneficiary's identity before proceeding
- Verify that the beneficiary is comfortable with the platform

During the call:

- Conduct the call from a private, professional environment



- Ensure the background is professional and appropriate
- Check that the beneficiary is in a safe and private environment (if appropriate)
- Be alert to signs of distress, coercion, or other concerns
- Do not record the call without explicit, written consent
- End the call immediately if safeguarding concerns arise

After the call:

- Record any significant information in the beneficiary's case file
- Report any concerns to the DSL immediately

7.4 Messaging Application Safeguarding Procedures

- Use only organisation-approved messaging applications with end-to-end encryption
- Use a dedicated organisation number, not a personal number
- Do not communicate with beneficiaries via messaging apps outside working hours (except in emergency)
- Be aware that messaging is not a secure method for sharing sensitive personal information
- Do not share images or documents without appropriate consent and security measures
- Report any concerning messages immediately to the DSL

7.5 Email Safeguarding Procedures

- Use your organisation email address only
- Use clear, professional subject lines
- Avoid sharing sensitive personal information in emails where possible
- Use encryption for sending sensitive documents
- Do not share other beneficiaries' personal information in emails
- Be aware that emails can be forwarded or shared without your knowledge
- Report any concerning emails immediately to the DSL

8

Social Media Policy and Procedures

8.1 Organisation Social Media Accounts

Ark of Hope Foundation For All Nations uses social media to promote our work, share news, engage with our community, and fundraise. Our organisation social media accounts are managed by designated staff members. Content is planned, approved and monitored.

8.2 Social Media Safeguarding Requirements

In line with the Charity Commission's updated social media guidance (April 2026) and the Online Safety Act 2023, we will:

- Maintain a Social Media Policy that reflects our obligations under the Online Safety Act 2023



- Moderate comments on our social media pages to identify and remove inappropriate, harmful or illegal content
- Direct safeguarding concerns raised via public social media channels to appropriate private channels rather than responding publicly
- Ensure our social media activity supports our charitable purposes, is in the charity's best interests, and complies with relevant laws and regulations
- Report harmful content to the platform provider where appropriate
- Consider risks before posting content that could put beneficiaries or staff at risk

8.3 Moderation Procedures

- Pre-moderation – where feasible, content is reviewed before posting
- Post-moderation – comments are reviewed regularly (at least daily)

Prohibited content includes:

- Comments that are abusive, threatening, or discriminatory
- Content that could identify a beneficiary without consent
- Spam, scams, or misleading content
- Content that is illegal or promotes illegal activity

Response protocol – inappropriate comments will be removed; persistent offenders may be blocked.

8.4 Staff and Volunteer Social Media Use

- Do not post about beneficiaries, colleagues or organisation matters on personal social media accounts
- Do not share organisation information that is confidential or not publicly available
- Be professional – personal social media use should not bring the charity into disrepute
- Do not engage in online arguments or discussions that could harm the charity's reputation
- Be aware that your personal social media activity may be seen by beneficiaries and others

8.5 Social Media and Beneficiary Privacy

- Photographs – we will only share images of beneficiaries with explicit, written consent
- Identification – we will not identify beneficiaries by name without consent
- Sensitive information – we will not share any personal or sensitive information about beneficiaries
- Consent can be withdrawn – beneficiaries can request removal of their image or content at any time

9

Remote Service Delivery – Detailed Procedures

9.1 Definition of Remote Service Delivery

Remote service delivery refers to any service provided by Ark of Hope Foundation For All Nations that is not delivered in person, including:

- Video calls and virtual support sessions
- Telephone support and counselling
- Online group activities and workshops
- Digital casework and advocacy
- Virtual drop-in sessions
- Online mentoring and befriending

9.2 Risk Assessment for Remote Service Delivery

Before delivering any service remotely, staff must conduct a risk assessment considering:

- The nature and sensitivity of the service being delivered
- The characteristics and vulnerability of the beneficiary
- The platform and technology being used
- The environment from which the staff member is delivering
- The environment from which the beneficiary is accessing the service

9.3 Safeguarding Procedures for Remote Service Delivery

Before the session:

- Confirm the beneficiary's identity
- Confirm the beneficiary's consent to the remote delivery method
- Agree on a private, safe location for the session (where possible)
- Ensure emergency contact details are available
- Have a clear procedure for managing distress or crisis remotely

During the session:

- Ensure you are in a private, professional environment
- Establish and maintain professional boundaries
- Be alert to signs of distress, coercion, or other concerns
- Do not conduct sessions while driving or in public places
- Do not share personal contact information
- End the session immediately if safeguarding concerns arise

After the session:

- Make a clear record of the session in the beneficiary's case file



- Report any concerns to the DSL immediately
- Follow up with the beneficiary as agreed

9.4 Emergency Procedures During Remote Sessions

- Immediate risk of harm – end the session and call 999 immediately
- Beneficiary in distress – provide support within your role; if unable to manage, seek guidance from DSL
- Technical failure – end the session and contact the beneficiary by phone to confirm they are safe
- Concern about staff safety – end the session and contact your line manager or DSL

10

Use of Personal Devices and Bring Your Own Device (BYOD)

10.1 Policy on Personal Device Use

Ark of Hope Foundation For All Nations recognises that staff and volunteers may use personal devices for work purposes. We encourage the use of organisation-provided devices where possible.

Where personal devices are used for work:

- Staff and volunteers must comply with all organisation policies
- Devices must have appropriate security measures (passwords, encryption, antivirus)
- Devices must be kept secure and not accessible to others
- Personal devices must not be used to store or share sensitive beneficiary data
- A personal device must not be used for work if it is shared with other family members
- Devices must be reported lost or stolen immediately

10.2 Security Requirements for Personal Devices

- A password or biometric lock (minimum 6 characters)
- Encryption enabled
- Antivirus and malware protection installed and updated
- Operating system and applications updated regularly
- Remote wipe capability (for lost or stolen devices)

10.3 Data Storage on Personal Devices

- Sensitive beneficiary data must not be stored on personal devices
- Data should be stored on organisation cloud platforms (e.g., Google Drive, OneDrive) where possible
- Downloaded files must be deleted after use
- Email attachments should be opened only in secure environments



11

Photography, Video and Image Sharing

11.1 Principles

Ark of Hope Foundation For All Nations is committed to protecting the privacy and dignity of our beneficiaries in all photography and video activity.

11.2 Consent

- Explicit, written consent must be obtained before taking or sharing any photograph or video of a beneficiary
- Consent must be informed – the individual must understand how the image or video will be used
- Consent must be freely given and can be withdrawn at any time
- Consent is required for each use of an image or video (e.g., for social media, website, fundraising materials)

11.3 Recording of Remote Sessions

- Remote sessions must not be recorded without explicit, written consent from the beneficiary
- Where consent is given, recordings must be stored securely and deleted when no longer needed
- Recordings must not be shared with third parties without additional consent

11.4 Use of Images

- Images will be used respectfully and not in a way that could cause distress or embarrassment
- Images will not be used in a way that could identify a beneficiary as experiencing a particular vulnerability without explicit consent
- Images will be stored securely and deleted when no longer needed

11.5 Mobile Phone and Camera Use

- Staff and volunteers must not use personal mobile phones or cameras to take photographs of beneficiaries unless authorised and with appropriate consent
- Organisation devices used for photography must be kept secure

12

Data Protection, Privacy and Information Sharing

12.1 Data Protection Principles

Ark of Hope Foundation For All Nations is committed to compliance with UK GDPR and the Data Protection Act 2018. In all digital activities, we adhere to the data protection principles set out in our Data Retention/Protection Policy:

- Lawfulness, fairness and transparency
- Purpose limitation



- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality
- Accountability

12.2 Data Security Measures

- Password policies – strong, unique passwords, changed regularly
- Two-factor authentication – required for accessing organisation systems
- Encryption – used for sending sensitive data and for stored data where appropriate
- Access controls – data accessible only to those who need it
- Secure storage – data stored on organisation-approved platforms
- Data disposal – data deleted securely when no longer needed

12.3 Information Sharing for Safeguarding

Our approach to information sharing is guided by the principles in Information Sharing: Advice for practitioners providing safeguarding services to children, young people, parents and carers (2018).

Key Principles:

- Necessary and Proportionate
- Relevant
- Adequate
- Accurate
- Timely
- Secure
- Recorded

Consent and Confidentiality:

- Safeguarding concerns will be handled confidentially, but confidentiality cannot be guaranteed where there is a risk of significant harm
- Information will be shared on a need-to-know basis with relevant agencies and individuals
- All information sharing will be in line with our Data Protection Policy and relevant legislation
- We will always seek consent from the individual before sharing information, unless doing so would place them or others at increased risk
- Where we share information without consent, we will document the reasons for doing so
- All staff are trained to seek consent where individuals may not expect their information to be shared



The right to confidentiality is not absolute. Sharing relevant information with the right people at the right time is vital to good safeguarding practice. All staff and volunteers can contact either the police or the local authority safeguarding lead for advice, without necessarily disclosing an individual's personal details, if they are uncertain whether a safeguarding referral would be appropriate.

12.4 Subject Access Requests

Beneficiaries have the right to access their personal data. All Subject Access Requests must be referred to the Data Protection Lead.

Data Protection Lead

Caroline Hinds

13

Online Safety Act 2023 – Compliance and Duties

13.1 Overview

The Online Safety Act 2023 places duties on providers of online platforms and services to keep people safe online. The Act applies to services that enable users to interact with each other, enable users to search for content, or are likely to be accessed by children.

13.2 Our Obligations

- Determine whether the Act applies – we will assess whether any of our digital platforms or services fall within the scope of the Act.
- Conduct risk assessments – if we operate any regulated service, we will carry out and maintain an up-to-date illegal content risk assessment and a children's access assessment.
- Implement safety measures – appropriate to protect against illegal content and harm to children.
- Maintain records – of our compliance with the Act.
- Comply with Ofcom guidance – to determine whether we are regulated under the Act.
- Update our Social Media Policy – to reflect how we comply with the Act.

13.3 Illegal Content Risk Assessment

Our illegal content risk assessment will consider the nature of the service and how it is used, the likelihood of users encountering illegal content, the potential impact of illegal content on users, and the effectiveness of our mitigation measures.

13.4 Children's Access Assessment

Our children's access assessment will consider the age range of users, the nature of content accessible to children, the risks to children from harmful content, and the effectiveness of age verification and other protection measures.



14

Working Together to Safeguard Children 2026 – Implications

14.1 Overview

The updated Working Together to Safeguard Children 2026 statutory guidance, published on 18 March 2026, sets out how organisations and agencies should work together to safeguard and promote the welfare of children. It applies to all organisations working with children, including charities.

14.2 Key Changes and Implications

Change	Implication for Ark of Hope Foundation For All Nations
Guidance applies to all children	Our safeguarding responsibilities apply to all children, regardless of their living circumstances.
Strengthened anti-racist and anti-discriminatory practice	We must challenge racism and discrimination in all our work, including digital contexts.
Strengthened guidance on online harms	We must recognise and respond to online harms as part of our safeguarding approach.
Recognition of multiple harms	Children may face multiple harms simultaneously; we must consider the whole picture.
Group-based exploitation	We must be alert to the risk of group-based exploitation, including in online contexts.
Reinforced organisational responsibilities	We have clear responsibilities to safeguard children in all settings.
Serious incident notifications	We must ensure serious incidents are notified to relevant agencies in a timely and accurate manner.

14.3 Our Commitments

- Applying the guidance – ensuring all staff and volunteers are aware of its implications for their roles.
- Anti-racist and anti-discriminatory practice – actively challenging racism and discrimination in all digital contexts.
- Online harms – recognising and responding to online harms as part of our safeguarding approach.
- Multiple harms – considering the potential for multiple harms in all safeguarding assessments.
- Partnership working – working effectively with local safeguarding partnerships.
- Serious incident notifications – ensuring these are reported to the Charity Commission and other relevant agencies in line with the guidance.



15

Reporting and Responding to Concerns – Detailed Procedure

15.1 Raising a Concern – Step-by-Step Guide

1 Listen

- Listen carefully to what the person is telling you
- Do not promise to keep secrets – explain that you may need to share information to keep people safe
- Let the person speak at their own pace; do not interrupt or ask leading questions
- Reassure the person that they have done the right thing by telling you

2 Do Not Investigate

- Do not try to investigate the concern yourself
- Do not ask detailed or leading questions
- Do not confront the alleged perpetrator
- Do not share the concern with others who do not need to know

3 Report Immediately

- Report the concern to the Designated Safeguarding Lead (Stella King) or the Deputy Safeguarding Lead (Deborah Newbould) in her absence, as soon as possible
- Report no later than the same working day
- If neither is available, report to a senior staff member or trustee
- If the individual is at immediate risk, call 999

4 Record

- Make a written record using the organisation's Safeguarding Report Template or Incident/Cause for Concern Template
- Record facts only, not opinions
- Include name, age, and contact details of the person at risk; nature of the concern; date, time and location (including digital platform used); name of any alleged perpetrator; any witnesses; a factual account of what was said or observed; any action taken; and the date and time of report to the DSL

5 Consult and Decide

You, your line manager, and the service user (where possible) will agree the next steps, which may include recording it as an incident and keeping it under observation, making a safeguarding referral to the Local Authority, or arranging additional support.



15.2 What to Record – Detailed Guidance

DO record

Factual observations, direct quotations, dates, times and locations, names and contact details, actions taken and by whom, any changes in behaviour observed, and the language used by the person at risk where relevant.

DO NOT record

Opinions or assumptions, speculation, unverified third-party information without attribution, or personal opinions about the alleged perpetrator.

15.3 Response and Referral – DSL Responsibilities

The Designated Safeguarding Lead will assess the concern, consult with relevant agencies (Stoke-on-Trent Safeguarding Children Partnership for child protection, Staffordshire and Stoke-on-Trent Adult Safeguarding Partnership Board for adult concerns, Staffordshire Police for criminal matters, LADO for allegations against staff or volunteers, and Ofcom for online safety concerns where applicable), make a formal referral where required, ensure the person at risk receives appropriate support, maintain a secure record of all actions taken, and report to the Board of Trustees as appropriate.

15.4 Making a Referral

Local authorities are the designated lead agencies with the duty to coordinate a response to allegations or concerns of abuse (under section 42 of the Care Act 2014 for adults, and under the Children Act 1989 for children).

Timescales for Reporting:

- Immediate action – if the person is at risk of serious physical harm or a serious criminal act has taken place and evidence needs to be preserved
- Within 24 hours – if it relates to a specific incident which may still be ongoing, or may happen again
- Within 7 days – for a more general concern that does not indicate immediate harm



Stoke-on-Trent Council (Adult Safeguarding)

Telephone: 0800 561 0015 (any time)
Minicom: 01782 236037
Email: social.care@stoke.gov.uk

Stoke-on-Trent Safeguarding Children Partnership (CHaD)

Telephone: 01782 235100 (office hours)
Out of hours: 01782 234234
Emergency: 999

Staffordshire & Stoke-on-Trent Adult Safeguarding Partnership Board

Write to: SSASPB Team, Staffordshire Place 1, Tipping Street, Stafford, ST16 2LP
Telephone: 01785 854071
Email: SSASPB.admin@staffordshire.gov.uk

Staffordshire County Council (Adult Safeguarding)

Mon–Thu: 0345 604 2719 (8:30am–5:00pm)
Fri: 0345 604 2719 (8:30am–4:30pm)
Other times: 0345 604 2886

Staffordshire Police

Emergency: 999
Non-emergency: 101

15.5 Emergency Situations

- Call 999 for police or ambulance
- Do not delay – ensure the person is safe
- Report to the Designated Safeguarding Lead as soon as possible afterwards
- Log any 999 calls using the Out of Hours Emergency number: 07956120599

15.6 ICE (In Case of Emergency) Card

All staff and volunteers should carry an ICE (In Case of Emergency) Card, a quick reminder of how to act in an emergency. This is covered in induction for new staff.

15.7 Historical Disclosures and Self-Inflicted Abuse

Historical Disclosures:

- Information about historical abuse must be relayed to the resident's Empowerment Worker
- Documented as a safeguarding disclosure or an Incident/Cause for Concern report, depending on severity
- Following consultation with line management, a decision will be made regarding escalation
- Historical abuse can also be reported to the non-emergency police line at 101 as anonymous intelligence

Self-Inflicted Abuse and Self-Neglect:

- Suspicion or disclosure of escalating self-abuse should be documented as an incident
- Concerns regarding a resident's deteriorating behaviour should be discussed with the assigned Empowerment Worker



- Any incidents of attempted suicide or serious contemplation of suicide should be promptly reported to relevant mental health teams
- If volunteers are the first responders, they should not hesitate to seek emergency assistance
- It is crucial to avoid leaving the individual alone until their safety is assured
- The resident's Risk Reduction Plan (RRP) should be reviewed and all safety measures reassessed

15.8 Concerns about a Colleague or Volunteer

- Report the concern to the Designated Safeguarding Lead
- If the concern relates to the Designated Safeguarding Lead, report to the Deputy Safeguarding Lead (Deborah Newbould, Chair of Trustees)
- Follow the organisation's Whistleblowing Policy where appropriate
- Do not confront the individual yourself
- Do not share the concern with others who do not need to know

16

Recording and Record-Keeping

16.1 Record-Keeping Principles

All safeguarding records will be accurate, timely, complete, secure and retained in line with data protection and retention policies.

16.2 What Records to Keep

- Safeguarding Report Templates
- Incident/Cause for Concern Templates
- Action logs
- Referral records
- Communication records
- Risk assessment records
- Training records
- Field notes

16.3 Storage and Security

- Stored securely, with access limited to those who need to know
- Stored in the organisation's SharePoint folder (accessible only to the Safeguarding Lead and Executive Director)
- Emails containing reports as attachments are deleted after saving to SharePoint
- Stored separately from general case files where appropriate
- Retained in line with our data retention policy and disposed of securely when no longer needed



- Ongoing or unfolding incidents are reported one month later using the template, with all parties remaining in contact for review and pastoral care

16.4 Confidentiality

All safeguarding records are confidential, shared only on a need-to-know basis, and handled in line with data protection legislation and safeguarding principles. Staff and volunteers should refer to the Confidentiality Policy and Data Retention/Protection Policy.

16.5 Bi-Monthly Sharing

Bi-monthly sharing of all safeguarding incidents and complaints takes place as part of quality assurance.

17

Allegations Against Staff or Volunteers

17.1 Policy Statement

Any allegation of abuse against a member of staff, volunteer or trustee will be taken seriously and handled in accordance with this policy and with guidance from the Local Authority Designated Officer (LADO) for child protection allegations, or the relevant adult safeguarding procedures.

17.2 Procedure

Stage 1: Immediate Action

- Report immediately to the Designated Safeguarding Lead
- DSL to consult with LADO (for children) or Adult Social Care (for adults at risk)
- Ensure the person at risk is safe

Stage 2: Investigation

- Consider suspension of the individual pending investigation (where appropriate)
- Full investigation in accordance with organisational disciplinary procedures
- Referral to relevant professional bodies (e.g., DBS) where appropriate

Stage 3: Support

- Provide support for the person at risk
- Provide support for the accused individual (where appropriate)
- Provide support for staff and volunteers affected by the allegation

Irrespective of the findings of social care or police inquiries, the Safeguarding Lead will assess all individual cases to decide whether a member of staff or volunteer can be reinstated and how this can be sensitively handled. The welfare of the child and young person remains of paramount importance throughout.

17.3 Referral to the Disclosure and Barring Service (DBS)

Where an individual has been dismissed or removed from their role because they have harmed or put at risk a child or adult at risk, we will make a referral to the Disclosure and Barring Service in line with our duty to refer.



17.4 Whistleblowing

Any staff member or volunteer who in good faith reports concerns that a colleague is, or may be, abusing a child or children will be fully supported and protected, in line with the Whistleblowing Policy.

17.5 Safer Recruitment

All prospective employees or volunteers who will be working alone with adults at risk undergo thorough vetting before being recruited, including self-disclosure of previous convictions at application, a conditional offer dependent on satisfactory references and DBS check, enhanced DBS checks for all staff and volunteers working with children, young people and adults at risk, DBS checks renewed every 3 years for all trustees, executives and staff working directly with residents, and supervised access until a satisfactory DBS check and references have been reviewed and verified.

18 Training and Awareness

18.1 Training Requirements

Role	Minimum Training Requirement
All staff and volunteers	Digital safeguarding awareness training as part of induction, with annual refreshers
Designated Safeguarding Lead	Specialist digital safeguarding training, including Online Safety Act and Working Together 2026
Deputy Safeguarding Lead	Specialist digital safeguarding training equivalent to the DSL, to ensure continuity of cover
Staff working directly with children	Enhanced training on online harms, grooming, and exploitation

18.2 Induction Training

All new staff and volunteers receive digital safeguarding training as part of their induction, covering this policy and its procedures, recognising signs of digital harm, how to report a concern, safe use of digital platforms, professional boundaries in digital contexts, data protection and privacy, and ICE Card procedures.

During the probationary period, all staff members are required to complete initial safeguarding training to ensure they understand their roles, our organisation's responsibilities, and how to recognise and respond to concerns effectively.

18.3 Ongoing Training

All staff and volunteers (and anyone offering resident support on behalf of Ark of Hope) receive refresher digital safeguarding training at least annually, tailored to their specific roles and responsibilities. Staff are expected to familiarise themselves with this policy, attend safeguarding



training offered locally or by Ark of Hope, attend annual refresher training, and undergo full safeguarding training every three years, or sooner if significant procedural changes occur.

18.4 Specialist Training

The Designated Safeguarding Lead and Deputy Safeguarding Lead receive additional specialist training, including managing safeguarding concerns and allegations, making referrals to external agencies, record-keeping and confidentiality, Working Together to Safeguard Children 2026, Online Safety Act 2023 duties, and digital safeguarding in the context of domestic abuse, modern slavery and No Recourse to Public Funds.

18.5 Training Records

Training records are maintained for all staff and volunteers, including date, type, trainer, completion status and renewal date.

18.6 Staff and Volunteer Support

Ark of Hope Foundation For All Nations acknowledges that abuse and safeguarding concerns are a difficult topic and will endeavour to support staff, residents, and volunteers throughout the process, including recommending external counsellors, a wellbeing check before a return to work, time off to rest where appropriate, a phased return where needed, and a completed 'back to work' report.

All staff should familiarise themselves with the Staff Care Policy and advice around returning to work after time off.

19 Monitoring, Evaluation and Review

19.1 Monitoring

This policy will be monitored through regular safeguarding reports to the Board of Trustees, review of safeguarding incident records, staff and volunteer feedback, audit of digital safeguarding practices, and bi-monthly sharing of safeguarding incidents and complaints.

19.2 Review

This policy will be reviewed annually by the Board of Trustees, following any safeguarding incident or near miss, following any significant change in legislation, guidance or organisational activity, and following any change in our digital activities or platforms. The Safeguarding Lead will attend safeguarding training every year.

19.3 Serious Incident Reporting

Any serious incident relating to digital safeguarding will be reported to the Charity Commission in line with their guidance. This includes a safeguarding incident resulting in significant harm, an incident reported to the police or other statutory agency, an incident receiving significant media



attention, or an incident resulting in the suspension or dismissal of a staff member or volunteer. Any major breach of policy by staff may require a Serious Incident report, escalated to Trustee level and potentially to the Charity Commission.

20 Related Policies and Documents

This Digital Safeguarding Policy should be read alongside the following related Ark of Hope Foundation For All Nations policies and documents:

Document	Purpose
Adult Safeguarding Policy	Core safeguarding policy covering all aspects of adult safeguarding
Child Safeguarding Policy	Core safeguarding policy covering all aspects of child safeguarding
Data Protection / GDPR Policy	Data protection, privacy and information sharing
Social Media Policy	Social media use and governance
Volunteer Policy	Volunteer recruitment, support and management
Whistleblowing Policy	Reporting concerns about wrongdoing
Code of Conduct	Behavioural expectations for staff and volunteers
Complaints Policy	Handling complaints from beneficiaries and others
Staff Care Policy	Staff wellbeing and support
Confidentiality Policy	Confidentiality and information sharing
Data Retention Policy	Data retention and disposal
Safer Recruitment and Selection Policy	Recruitment procedures
DBS Policy	DBS check procedures
Missing Persons Policy	Responding to missing persons
Child Sexual Exploitation Policy	Identifying and managing CSE concerns
Health and Safety Policy	Health and safety in the workplace

21 Approval and Sign-off

This Digital Safeguarding Policy has been approved by the Board of Trustees of Ark of Hope Foundation For All Nations.



Chair of Trustees

Date: _____

Designated Safeguarding Lead

Date: _____

Document Control

Policy Owner	Designated Safeguarding Lead
Approved By	Board of Trustees
Date Approved	
Next Review Date	

Version History

Version	Date	Author	Changes
1.2	18 August 2026		Confirmed Deborah Newbould as Deputy Safeguarding Lead; removed all Safeguarding Lead Trustee references; updated 15.8 escalation route accordingly



A

Appendices

A

Safeguarding Report Template

Reference the existing Safeguarding Reporting Template (Appendix 1 of the Adult Safeguarding Policy).

B

Incident or Cause for Concern Report Template

Reference the existing Incident or Cause for Concern Report Template (Appendix 2 of the Adult Safeguarding Policy).

C

Contact Details for Safeguarding Reporting

Ark of Hope Foundation For All Nations Safeguarding Lead

Stella King, Project Lead
Telephone: 07956120599
Email: info@arkofhopefoundation.com

Deputy Safeguarding Lead

Deborah Newbould, Chair of Trustees

Stoke-on-Trent Council (Adult Safeguarding)

Telephone: 0800 561 0015 (any time)
Minicom: 01782 236037
Email: social.care@stoke.gov.uk

Stoke-on-Trent Safeguarding Children Partnership (CHaD)

Telephone: 01782 235100 (office hours)
Out of hours: 01782 234234
Emergency: 999

Staffordshire & Stoke-on-Trent Adult Safeguarding Partnership Board

Write to: SSASPB Team, Staffordshire Place 1,
Tipping Street, Stafford, ST16 2LP
Telephone: 01785 854071
Email: SSASPB.admin@staffordshire.gov.uk

Staffordshire County Council (Adult Safeguarding)

Mon–Thu: 0345 604 2719 (8:30am–5:00pm)
Fri: 0345 604 2719 (8:30am–4:30pm)
Other times: 0345 604 2886

Staffordshire Police

Emergency: 999
Non-emergency: 101

D

ICE (In Case of Emergency) Card

Reference the existing ICE Card template (Appendix 6 of the Adult Safeguarding Policy).

E

Guidance on Mental Capacity

Reference the existing Guidance on Mental Capacity (Appendix 5 of the Adult Safeguarding Policy).



F

Body Map

Reference the existing Body Map (Appendix 4 of the Adult Safeguarding Policy) for recording physical injuries observed during digital safeguarding concerns.

G

Flowchart for Responding to a Child Safeguarding Concern

Reference the existing flowchart (Appendix 2 and 3 of the Child Safeguarding Policy).