Digital Safeguarding Policy

POLICY DOCUMENT VERSION: 2

POLICY DOCUMENT AUTHOR: HELEN DAVIES / DESIGNATED SAFEGUARDING LEAD

LAST REVIEWED: 29 NOVEMBER 2024

APPROVED BY: CHAIR AND BOARD OF TRUSTEES

NEXT REVIEW DATE: 1 DECEMBER 2025

1.Policy Statement

The Family Centre Deaf Children (FCDC) is committed to promoting the welfare of children, young people and adults at risk and to safeguarding them from harm in all its forms.

In today's digital age, the internet and digital technologies are an integral part of our lives, and they present a range of risks and challenges to children, young people and adults at risk.

We are committed to ensuring the digital safeguarding of children, young people and adults at risk, and to implementing best practice in this area.

This policy outlines FCDC's expectations for the appropriate use of digital media by FCDC staff, volunteers, partners, representatives, supporters, project participants and service users/beneficiaries – as well as anybody who comes into contact with us through digital platforms, including children, young people and adults at risk.

FCDC has a zero-tolerance policy towards power abuses and sexual harassment, exploitation and abuse, whether this takes place in the online or offline sphere.

FCDC is committed to:

- supporting victims/survivors of abuse/violence
- improving the charity's safeguarding capacity and practice
- reporting, investigating, responding to and preventing power abuses and sexual harassment, exploitation and abuse.

This policy complements FCDC's existing safeguarding policies and Data Protection and Confidentiality Policy.

This policy should also be guided by FCDC's Codes of Conduct.

2. Purpose and Scope

The purpose of this policy is to:

- Ensure that children, young people and adults are kept safe from harm when interacting digitally with FCDC.
- Provide FCDC staff and volunteers with the overarching principles that guide our approach to digital safety.
- Ensure that, as an organisation and as individuals, we operate in-line with our values an within the law in terms of how we use digital devices and services.

This policy sets out FCDC's approach to digital safeguarding and covers all digital spaces where FCDC's work is conducted. This includes (but is not limited to) emails, internal and external social media channels and online platforms relating to FCDC's work, including Facebook, X, Instagram, WhatsApp, LinkedIn, websites, internet services and ICT equipment provided by FCDC.

This policy aims to ensure that the use of digital technologies by children, young people and adults at risk is safe, responsible and appropriate, and that our staff and volunteers understand and implement best practice in digital safeguarding.

This policy applies to all staff, volunteers, sessional workers and third-party contractors who work with children, young people and adults at risk on behalf of FCDC and who use digital technologies as part of their work.

The guidance in this policy should not be taken as an exhaustive list. As the digital world rapidly evolves, it is important that FCDC staff, volunteers and others working on our behalf take responsibility for considering the full range of risks and safeguards required.

3. Principles

The Family Centre (Deaf Children) is committed to the following principles of digital safeguarding:

i. *Empowerment* – we will empower children, young people and adults at risk to understand and use digital technologies safely and responsibly, and to make informed choices about their online activity.

ii. *Prevention* – we will take steps to prevent harm to children, young people and adults at risk through the use of digital technologies, including by identifying and responding to risks and vulnerabilities.

iii. *Protection* – we will protect children, young people and adults at risk from harm through the use of digital technologies, including by ensuring that appropriate security measures are in place, and that access to personal data is restricted.

iv. *Partnership* – we will work in partnership with parents/carers, other professionals, and the wider community to ensure that children, young people and adults at risk are safe online.

v. *Responsibility* – we will ensure that all staff and volunteers take responsibility for digital safeguarding, and that they are aware of and comply with this policy

4. Digital Safeguarding Commitment

It is FCDC's responsibility to ensure the health, safety and wellbeing of staff, partners, volunteers, project participants and service users. Based on systematic feedback mechanisms, it is FCDC's responsibility to monitor this and to take appropriate measures when necessary.

4.1 FCDC's safeguarding commitment is to:

- Create and maintain a safe organisation culture for our beneficiaries, staff, volunteers and others working on our behalf.
- Ensure everyone associated with the delivery of our work has access to information about how to report safeguarding concerns or allegations of abuse or exploitation.
- Ensure that all concerns or allegations of sexual harassment, exploitation, neglect and abuse are responded to in a timely and appropriate manner and that there are multiple channels through which people can raise concerns.
- Ensure zero tolerance of sexual harassment, exploitation and abuse in the organisation through robust prevention and response work, offering support to victims/survivors and holding those responsible to account.
- Adopt an approach that respects the confidentiality and decision-making rights of victims/survivors where possible and appropriate to do so.

- Build a culture where all those we work with and who work for FCDC feel empowered to insist on non-discriminatory and respectful behaviour from each other, where poor behaviour is not accepted, and where power is not abused.
- Be transparent about safeguarding issues occurring within FCDC, in line with privacy regulations and within legal frameworks.
- Be sensitive in our communications about our practices and open to learning and improving.
- Ensure everyone associated with the delivery of our work will have access to, and be familiar with, the charity's safeguarding policies/procedures and know their responsibilities within them.
- Ensure everyone who works on behalf of FCDC with children and vulnerable populations receive regular training in relation to child, young people and adult safeguarding.
- Ensure staff and volunteers with specific safeguarding responsibilities at FCDC receive additional training commensurate with their role.

4.2 FCDC's digital safeguarding commitment is to:

- Support everyone involved in FCDC's work to navigate digital spaces and use equipment and digital tools safely and effectively.
- Be proactive in promoting digital safety by providing guidance, tools and training to our staff and volunteers.
- Take appropriate action on digital safeguarding and data protection incidents when FCDC is aware of these.

5. What is Digital Safeguarding?

Digital safeguarding means: *protection from harm in the online environment through the implementation of effective technical solutions, advice, support and procedures for managing incidents*.

Digital safeguarding at FCDC means protecting our service users/beneficiaries, staff, volunteers, sessional workers and others working on behalf of the charity from online harms such as:

- **Cyberstalking** – Repeatedly using electronic communications to harass, intimidate or frighten someone. For example, by sending threatening messages.
- **Discrimination and 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 wrong 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** – Where someone pretends to be someone else online. This is often by taking photos from social media to build a fake profile. This is sometimes known as ‘catfishing’.
- **Misinformation** – Where someone shares information they think is correct, but it isn’t.
- **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.
- **Promotion of self-harm, suicide and eating disorders** – Content encouraging these harmful behaviours on social media.
- **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 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/tactics 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.
- **Oversharing personal information** – This includes information that makes someone identifiable, like their names or phone number. It may also include identifying details based on someone’s protected characteristics.

6. Digital Safeguarding Risks

The following risks should be taken into account when considering digital safeguarding:

6.1 Content risks

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 according to national laws, e.g. sexually exploitative images of children or radicalising videos. Inappropriate and offensive content is more subjective, and includes: 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/expression, sexual orientation, (dis)ability, religion, language or other status.

6.2 Contact risks

Risks that are produced as a result of the online behaviour of other people. 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, but not limited to:

- Bullying online or through mobile phones

- Coercive control - an act or a pattern of acts of assault, threats, humiliation and intimidation or other abuse that is used to harm, punish, or frighten their victim.
- Harassment and stalking
- Ideological grooming
- Exposure to political risk, e.g. government surveillance or having details of online activism shared with authorities in politically oppressed contexts
- Increased exposure to cybersecurity risks, e.g. by having malicious content shared such as ransomware, apps or other active content or malicious code
- 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
- Distribution of private and sexual images, e.g. the distribution of sexually exploitative images or videos without an individual's permission
- 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

6.3 Conduct risks

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 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.

6.4 Technology-based gender-based violence

FCDC recognises that online harassment, bullying and sexual exploitation can affect anyone, but is most likely to affect women, girls and LGBTQI+ individuals. These groups face an increased risk of violence through digital technology, which can be considered a form of Gender-Based Violence.

FCDC staff, volunteers, sessional workers and others working on behalf of FCDC should be aware of common perpetrators and acts of such abuse/violence.

Perpetrators include:

- Individuals or groups who target people on an ideological basis such as fundamentalist, patriarchal, sexist or homophobic groups.
- Organisations who find gender justice or LGBTQI+ rights work threatening to their power and authority.
- Acquaintances, intimate partners or family members who wish to harm someone or exercise power over them.

Acts of abuse/violence include:

- Online harassment and trolling.
- Cyberstalking (tracking and monitoring of someone's movements and activities online).

- Invasion of privacy by gaining access to phones, devices, and email or other accounts without consent.
- Distribution without consent of private and sexual images, or using these images as leverage and enforcement of power dynamics.

7. Use of Equipment, Internet and Social Media

All FCDC staff and volunteers must adhere to FCDC's Codes of Conduct and the guidelines detailed below when using equipment, internet, social media or digital platforms on behalf of, or belonging to, FCDC.

FCDC should carry out a Risk Assessment for all initiatives involving social media or digital platforms or where FCDC is providing equipment or internet. Special consideration should be taken where these initiatives involve children, young people and vulnerable adults, and monitoring of usage may be appropriate.

Where significant risk may exist to individuals (risk of harm, distress, or the infringement of other rights and freedoms), there may be an explicit legal requirement to carry out a Privacy Impact Assessment (PIA). The Risk Assessment may be carried out in conjunction with a PIA, or may itself be a PIA.

7.1 Use of FCDC's internet and ICT equipment

- It is prohibited for anyone to browse, download, access or share content which is illegal, harmful, violent, extremist, sexually exploitative, abusive, offensive or otherwise inappropriate using equipment or internet which has been provided by FCDC, unless this is required for their role e.g. safeguarding and investigator roles.
- Parameters for acceptable usage of equipment will be set by FCDC, and FCDC may use software to limit applications or online tools staff, volunteers, sessional workers, contracted professionals or service users are able to access.
- Equipment provided by FCDC should ensure that technical solutions are in place to protect the user, e.g. anti-virus, monitoring and filtering software.
- Appropriate monitoring should take place based on the level of risk of the people involved (e.g. children, young people, vulnerable adults), and the content which they will be coming into contact with.
- FCDC should give advice, support and training in how to mitigate risk when using equipment and internet which it has provided.
- Where FCDC is providing equipment to a service user, sessional worker, project participant/partner, or others involved in FCDC's work, equipment should be cleaned of any personal data at the end of a project or partner assignment. When allocating equipment to an individual, it must be made clear to them that they are now responsible for the use of the equipment.

7.2 Use of Social Media and Digital Platforms

- Staff, volunteers and others working with FCDC are personally responsible for what they communicate on social media and digital platforms, and when using FCDC's internet and equipment, both on behalf of FCDC and in a personal capacity. Published content is often available for anyone to read, and may

reflect negatively on the organisation, while those using online platforms as part of FCDC's work may be exposed to harmful content.

- Staff, volunteers and others working on behalf of FCDC should not behave in a threatening, bullying or abusive way online – whether in a professional or personal capacity

- FCDC's Centre Manager is responsible for signing off the creation of official social media accounts or digital platforms related to FCDC's services, events, campaigns or initiatives, and accounts and platforms should not be developed without the Centre Manager's sign-off.

- Staff responsible for the creation of online content on FCDC accounts, website and platforms (e.g. Instagram and Facebook posts) should seek advice and sign-off from the Centre Manager if they are concerned about the appropriateness or nature of the content.

- Children and vulnerable adults should not be tagged in any online or social media posts.

- If illegal, harmful, violent, extremist, sexually exploitative, abusive, offensive or otherwise inappropriate content is posted in FCDC's groups or platforms, this should be deleted or hidden by a staff member and where appropriate reported to third-party platform hosts. If FCDC staff, volunteers ot representatives see or are made aware of such content, but do not have administration rights to remove it, they should report it to the Centre Manager following the procedures outlined in Sections 12 and 13 below.

- FCDC initiatives using social media should be aware of age limits for corresponding social media platforms (e.g. a campaign using Facebook as a key promotion tool should be aware that the minimum user-age is 13).

- If an online profile, group, page or platform is set up directly related to FCDC's services, events or initiatives, a minimum of two members of FCDC staff should oversee the content and activity as 'moderators'. Moderators should remove or edit inappropriate content as soon as possible after it has been posted and should set up mechanisms to pre-approve content where this is enabled by the third-party provider.

- Staff and volunteers should not make use of their personal social media accounts to carry out FCDC-related work, projects, events or initiatives.

- FCDC staff can only use their FCDC email address to set up social media accounts if these accounts will be used on behalf of the organisation. Where this account represents an FCDC initiative, managers should have access to this account, and login details should be shared with other staff members so that this account can be used as a shared resource.

- FCDC staff, volunteers and others working on behalf of the charity should not have private conversations with anyone under 18 years old through email, or through accounts on social media or online platforms where these are not official FCDC accounts.

- Where children contact FCDC through the charity's official social media or online platform accounts, e.g. to ask for more information about a project, processes should be in place so that at least two other

staff members are able to view these messages, and are informed when a message is sent to or received from a child.

In other instances, if sending a direct message to a child is unavoidable, e.g. to inform them of a sudden change to a planned FCDC event or activity, an adult with a duty of care towards the child (e.g. parent, guardian or teacher) and a relevant FCDC staff member (e.g. manager) should be copied into the message.

- FCDC should provide guidelines on settings and privacy to people engaging in digital spaces for FCDC initiatives to protect them from harmful behaviours.

- Sharing online content of people involved in FCDC's work on social media should follow FCDC's guidelines and policies on privacy, data protection, image/information sharing and confidentiality.

8. Privacy, Data Protection and Informed Consent

8.1 Privacy and Data Protection

FCDC has a duty of care to protect the digital data and content of staff, partners, representatives, volunteers, supporters, project participants, beneficiaries and others involved in FCDC's work, even when they make the informed decision to share this content. This duty of care is rooted in privacy law and includes an obligation to be transparent in explaining how FCDC will use individuals' data, how FCDC considers the risk to individuals, and how FCDC cares for their data throughout the lifespan within which it will be used.

FCDC must take every reasonable precaution to ensure that any digital data or content does not place people at risk or render them vulnerable to any form of harassment, abuse or exploitation.

Research which involves digital elements, such as online surveys or platforms, must be well thought through and appropriate for the context. Special consideration must be given to data protection concerns and mitigating risk to research participants.

FCDC staff, volunteers, sessional workers and others working on behalf of the charity must adhere to FCDC's Data Protection and Confidentiality Policy. All information stored digitally and online by FCDC must be processed in accordance with this policy and reflect any national laws on which this policy is based, such as the General Data Protection Regulation (GDPR).

Any digital activities must embrace the following principles at a minimum, which align with GDPR:

- FCDC is transparent, lawful, and fair with individuals when using their data, and will explain to individuals how it will use data when it collects or obtains it.
- FCDC will only use data for the purposes for which it was obtained and then destroy it appropriately.
- FCDC will not retain or use this information to contact or work with people for any other reason.
- FCDC will only collect the minimal amount of data for the purpose at hand.
- FCDC will retain accurate data and keep it for no longer than necessary.
- FCDC will ensure its data is stored securely and access is restricted to as small a number of staff as possible.

- FCDC will always seek written parental consent prior to collecting and using data related to children. The consent form must be sensitive to children, it must stipulate what channels the content will be used on, and it must outline that social media content will exist indefinitely unless the parents or child ask for it to be deleted.
- FCDC will only disclose personal information outside of FCDC in an identifiable form if explicit consent has been given for this or there is a compelling legal reason (or similar overriding interest) which is considered and risk-assessed.
- FCDC will comply fully with all data protection legislation.
- FCDC will ensure that all projects and activities which involve data must include planned consideration for the protection of confidentiality of data (security) and the privacy and agency of individuals (privacy).

8.2 Informed Consent

FCDC should ensure that informed consent is obtained for the gathering of content which will be shared publicly in the digital sphere. This should ensure that the person truly understands what they are consenting to, with full knowledge of the possible risks and benefits.

Privacy and data protection laws which outline the legal requirements for gathering and using data may in some instances require or present an option for consent, and these should be considered alongside FCDC's guidelines for gathering and sharing content online as detailed below.

FCDC guidelines for gathering and sharing content online:

- For children, FCDC must seek informed consent from a parent or guardian, in addition to attaining informed consent from the child, where they are old enough to understand.
- Adults, children's parents/guardians, and – where possible – children must be given enough context to make this context 'informed'. In particular, they must be able to reasonably understand how their image or likeness may be used, and what the consequences may be.
- Images, stories, recordings or other personal data of children should not be accompanied by identifying information when shared online, e.g. the child's real name or school name. This applies even if a parent/guardian gives informed consent for a child to be interviewed in a way that reveals their identity. Exceptions can only be made in specific circumstances, e.g. where a child has won a prize or led a campaign and this has been widely reported in the media, where a full Risk Assessment has been carried out and the identified risks are minimal, and where informed consent is obtained following this Risk Assessment.
- Identifying information should not be included when content is shared online where this may put people at risk, e.g. political harassment, targeting by religious extremists.
- A story-gatherer (e.g. interviewer, photographer, video-maker) 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.
- Everyone retains the right to remove any pictures or stories about them from FCDC online spaces at any stage and should be made aware of this.

  There must be a practical means for adults, children's parents/guardians - and where possible - children to contact FCDC to allow them to assert this right.

- Content should receive the appropriate levels of manager sign-off when gathering content and before sharing it online.
- There are some key areas where FCDC needs to be extremely alert and sensitive to sharing content online as there may be additional risk, and this may be ongoing:
  - Emergency situations – vulnerable, traumatised individuals
  - Abuse – survivor of any form of abuse
  - Crime – perpetrators or survivors of a crime

9. Children and Young People

FCDC recognises that children and young people experience specific risks in the digital sphere, and that special measures should be taken to ensure that they are protected from abuse, harm and exploitation when engaging with FCDC's online work and activities.

Special considerations include:

- FCDC should obtain informed consent from the child and/or parent or guardian of the child for the processing of children's data. An explanation of how the data will be used must be provided.
- FCDC guidelines on informed consent and identification of children must be followed when gathering content to share publicly (see Section 8.2 above for more information).
- FCDC should not support children to engage in FCDC's work through social media or digital platforms when they are under the minimum joining age set by the third-party provider.

  It is FCDC's responsibility to be aware of minimum age requirements, which vary across third-party platforms (e.g. on Facebook the minimum user-age is 13).

  For children over the minimum joining age, a Risk Assessment should determine whether social media platforms are the most appropriate way for FCDC to engage with them.
- FCDC should provide guidance and tools to children and young people to protect themselves when using equipment, internet, social media or digital platforms to work and engage with FCDC.
- Appropriate training should also be provided where possible. This includes (but is not limited to) social media privacy settings, online security, sharing content, and engaging with others online.
- The use of technical equipment, internet, social media or digital platforms not only carries individual and technical risks, but also collective and social risks that could increase the gap between people that have access to the digital world and those who do not. It can also push young people into groups and promote polarisation, which is particularly relevant for young people who are forming their identities. Whenever FCDC engages with young people in a way that includes digital work, these elements should be considered and discussed with young participants.
- FCDC personnel working with children and young people should also refer to FCDC's Children and Young People Safeguarding Policy and Code of Conduct: when working with children and young people.

10. Roles and Responsibilities

Safeguarding is everyone's responsibility. Everyone who works for and on behalf of FCDC is required to report any digital and non-digital safeguarding suspicions, concerns or incidences (see sections on reporting below).

- **FCDC's Board of Trustees** hold overall accountability for this policy and its implementation.
- **FCDC's Designated Safeguarding Trustee** is responsible for:
  - Championing safeguarding across the organisation.
  - Ensuring the organisation's risk register reflects safeguarding risks properly and sensible measures are in place, including relevant insurance for trustees liability.
  - Attending relevant safeguarding meetings, training events and conferences.
  - Supporting the trustees in developing their individual and collective understanding of safeguarding.
  - Working with the Designated Safeguarding Lead in order to manage all serious safeguarding cases.
  - Supporting regular safeguarding updates for staff, volunteers and beneficiaries.
  - Ensuring ways of gathering the views of staff and volunteers in relation to safeguarding and sharing these with the board. overseeing the implementation of this policy
  - Ensuring there is an annual review of safeguarding policies and procedures and that this is reported to trustees.
  - Monitoring whether policies and procedures are effective.
  - Learning from case reviews locally and nationally, to improve FCDC's policies, procedures and practices.
  - Overseeing safeguarding allegations against staff and volunteers, together with the Designated Safeguarding Lead.
  - be a point of contact for staff or volunteers if someone wishes to complain about a lack of action in relation to safeguarding concerns.
  - Deputising for the Designated Safeguarding Lead when absent or unavailable.
- **FCDC's Designated Safeguarding Lead (DSL)** is responsible for:
  - The implementation and review of this policy
  - Preventing and responding to digital safeguarding concerns
  - Raising awareness of this policy and promoting safeguarding best practices
  - Receiving and responding to concerns
  - Conducting referrals to specialist safeguarding services and supporting investigations.
  - Providing support to staff and volunteers to help implement this policy
  - Providing safeguarding information and guidance
  - Ensuring all staff and volunteers receive regular safeguarding training at a level appropriate to their roles and responsibilities.
  - Attending regular safeguarding training at the appropriate level.
  - Ensuring, where practical, there are systems in place to facilitate the monitoring of digital safety within the charity and that they receive reports on any breaches of this policy.
  - Ensuring that staff and volunteers are aware of the procedures that need to be followed in the event of a digital safeguarding incident taking place

- Keeping up to date with developments in digital safety and safeguarding.
- Reporting to the Board of Trustees on safeguarding incidents and issues

- **FCDC managers are responsible for** promoting awareness of this policy to the people they manage and for supporting and developing systems that create and maintain a safe working and service delivery environment. This includes the responsibility for ensuring the staff and volunteers who they manage receive regular safeguarding training at a level appropriate to their roles.
- **FCDC's Centre Manager is responsible for**:
  - Carrying out risk assessments at FCDC, including digital risks
  - Signing off the creation of official FCDC online accounts and platforms, and for coordinating sign-off of sensitive content as necessary.
  - Ensuring that all information stored digitally and online by FCDC is processed in accordance with FCDC's Data Protection and Confidentiality Policy and relevant laws on which these policies are based.
- **Staff and Volunteers are responsible for ensuring that they**:
  - Have read and understood FCDC's Safeguarding Policies, Procedures, Codes of Conduct and Digital Safeguarding Policy.
  - Adhere to the behaviours and processes outlined in this policy when carrying out their work or volunteering activity.
  - Report any suspected misuse or abuse to the DSL/DST in-line with FCDC Safeguarding Procedures.
  - Make sure that digital communications with children, young people and adults are appropriate and do not put people at risk of harm.
- All key stakeholders will be responsible for enhancing this policy and incorporating lessons learned into subsequent versions. Feedback from stakeholders will be sought in the process.
- Failure to report online and offline safeguarding concerns and incidents to the charity's Designated Safeguarding Lead is a breach of FCDC's safeguarding policies and could lead to disciplinary action being taken against employees and the termination of volunteer agreements and FCDC's relationship with other non-employees.
- There is no obligation for an individual to report any incident that has happened to them.

11. Procedures

The Family Centre (Deaf Children) will implement the following procedures to ensure digital safeguarding:

i. Risk assessments – we will carry out risk assessments to identify potential risks and vulnerabilities associated with the use of digital technologies by young people and adults at risk, and we will take steps to mitigate these risks.

ii. Consent and parental/carer involvement – we will obtain appropriate consent from children, young people and adults at risk for their use of digital technologies, and we will involve parents/carers as appropriate.

iii. Training and support – we will provide appropriate training and support to staff and volunteers to enable them to implement best practice in digital safeguarding.

iv. Monitoring and reporting – we will monitor the use of digital technologies by children, young people and adults at risk, and we will respond appropriately to any concerns or incidents of harm.

v. Confidentiality and data protection – we will ensure that all personal data is stored and processed in accordance with the Data Protection Act 2018 and the General Data Protection Regulation (GDPR).

vi. Reporting and escalation – we will have clear procedures in place for reporting and escalating concerns or incidents of harm associated with the use of digital technologies by children, young people and adults at risk, including referral to the appropriate authorities.

12. How to Raise a Complaint or Concern

Anyone can raise a concern about inappropriate or illegal content which has been posted online relating to FCDC's services and activities.

Digital content concerns should be raised with social media, website, channel, shop, project, programme and FCDC managers as appropriate, so that they can moderate and remove this content and report to a third-party service provider.

In the case of illegal content or a safeguarding concern, this should be raised with FCDC's Designated Safeguarding Lead, so that they can deal with this appropriately and refer to the police or a support service where necessary.

FCDC staff, volunteers and others working on behalf of the charity have a responsibility to report any suspicion or concerns about digital safeguarding.

Any individual can raise a concern/complaint to FCDC about an incident they have experienced, witnessed, or heard about concerning an FCDC staff member, volunteer or partner (suppliers, project partners, contractors, etc.) without fear of retribution.

FCDC staff and volunteers MUST NOT investigate allegations or suspicions themselves.

Issues relating to data protection and privacy should be reported to FCDC's Data Protection Officer. (See Annex 1 for contact details)

13. How to Respond to a Complaint or Concern

FCDC is committed to responding to all complaints and concerns relating to safeguarding (online and offline).

If you have a concern or complaint, contact The Centre Manager who is the Designated Safeguarding Lead (DSL) at FCDC and is responsible for:

- safeguarding concerns and complaints
- moderating and removing inappropriate online content and flagging this with third-party providers where appropriate.
- establishing if a copy or screenshot of the online content should be saved for use in future internal or external investigations.

- contacting third-party providers to report content concerns and issues.

The DSL has specialist expertise in prevention of and response to exploitation and abuse, including referrals for assistance and investigation. Please see Annex 1 for Safeguarding Lead contact details.

FCDC recognises that disclosures and suspicions should always be acted upon swiftly. If there is an urgent safeguarding situation, e.g. a supporter, project participant or beneficiary shares online that they are in imminent danger of harm or abuse, then immediate protective action must be taken. The DSL should be contacted immediately in these instances and all reasonable measures should be taken to prevent harm/abuse occurring. e.g. by contacting the police or appropriate support service directly where possible.

Please refer to FCDC's Safeguarding Policies and Procedures for further information on responding to and reporting safeguarding suspicions, concerns and allegations.

14. Policy Breaches

Breaches of this Policy may result in disciplinary procedures, change of duties, termination of employment or relationship, and possible legal proceedings, for FCDC staff, contractors, volunteers or people working in FCDC's name.

FCDC will take action against anyone, whether they are the subject of a complaint or not, who seeks to or carries out retaliatory action (such as, but not limited to, harassment, intimidation, unfair disciplinary action or victimisation) against complainants, survivors or other witnesses. Employees who are found to do this will be subject to disciplinary action, up to and including termination of employment.

Others who work with FCDC may have their relationship with FCDC terminated.

If an FCDC employee is found to have made an allegation that they knew to be false, they will be subject to disciplinary action, up to and including termination of employment.

Others who work on behalf of FCDC will be subject to action that may result in the termination of their relationship with FCDC.

15. Support for Victims Survivors

Victims/survivors are entitled to specialist support services. FCDC commits to referring victims/survivors to relevant specialist support services as appropriate and available and according to the wants and the needs of the victim/survivor.

Support may include specialist psychosocial support such as counselling, medical assistance, legal counselling and access to FCDC's Employee Assistance Programmes (where available).

16. Policy Review

FCDC will review and update this policy annually to ensure that it remains current and effective.

Annex 1

FCDC Safeguarding and Data Protection Contacts

Designated Safeguarding Lead (DSL)	Contact Helen immediately with any safeguarding concerns, queries or allegations.	**Helen Davies** Centre Manager Tel:01179030366 Email: helen@fcdc.org.uk
Designated Safeguarding Trustee (DST)	Contact Neil with any safeguarding concerns/issues if you cannot reach Helen or if you have a concern or allegation about the DSL (Centre Manager).	**Neil Curry** Chair (Board of Trustees) Tel:07946733033 Email: neil@fcdc.org.uk
Data Protection Officer	Contact Helen immediately with any data protection or privacy concerns, queries or allegations.	**Helen Davies** Centre Manager Tel:01179030366 Email: helen@fcdc.org.uk

Annex 2

For the purposes of this Policy and FCDC's approach to Digital Safeguarding, these definitions apply.

Adult: anyone aged 18 years or over.

Adult at risk: someone aged 18 or over with needs for care and support who is at risk of or is experiencing abuse and is unable to protect themselves as a result of their need for care and support.

Allegation: is a claim made about someone that they have acted inappropriately, are abusing a child or adult or are putting them at risk of abuse or harm. It may include "low-level concerns" where there is no clear evidence of abuse or harm, but the behaviour is in breach of FCDC's Code of Conduct and falls short of standards expected by FCDC.

Data protection: The process of protecting the rights and freedoms of individuals in respect of the use of their Personal Data. "Personal Data" means any information relating to an identified or identifiable natural person (a "data subject"). FCDC has an obligation under applicable privacy and data protection laws to protect the personal data which it collects and processes.

Child: A child is defined as anyone under 18 years old. This definition is recognised internationally as identifying a population who are particularly vulnerable and require additional safeguards to protect their rights. The definition of a child for the purposes of safeguarding should not be confused with the legal definition of a child or age limits set out in other relevant laws. The fact that a young person under the age of 18 may have reached the age of e.g. sexual consent, voting age etc. does not alter their inherent vulnerability as a child.

Young Person: FCDC defines a young person as being between the ages of 15 and 24, in line with the UN definition. When using the term youth or young people, we recognise that young people are not a homogeneous group and experience different levels of privilege and marginalisation that should be taken into account.

Vulnerable adult: A vulnerable adult is any person aged 18 years and over who is or may be in need of community care services by reason of mental health issues, learning or physical disability, sensory impairment, or unable to protect themselves due to age or illness and who may be unable to take care of themselves or unable to protect themselves against significant harm or serious exploitation. This includes people encountering domestic abuse, substance misusers and asylum seekers. An elderly person, while they may require extra support, does not necessarily meet the definition of adult at risk.

Safeguarding: is the action that is taken to promote the welfare of children and adults at risk to protect them from harm.

Safeguarding children is defined as:

- Protecting children from abuse and maltreatment
- Preventing harm to children's health or development
- Ensuring children grow up with the provision of safe and effective care
- Taking action to enable all children and young people to have the best outcomes

Safeguarding adults means protecting their rights to live in safety, free from abuse and neglect.

Safeguarding concern: is where a child or adult is being abused or is at risk of abuse. This concern may arise through what is observed, heard or told (a disclosure) including information or images shared digitally.