The Engineering Development Trust
Online Safeguarding Policy

Safeguarding Principles for Online Engagement Activities

*To be read in conjunction with EDT's Safeguarding Policy

This policy provides guidance on how EDT uses the internet and social media and the procedures for doing so. It also outlines how we expect the staff and volunteers who work for us.

Safeguarding is everyone's responsibility.

Designated Safeguarding Lead (DSL) - **Ciara Duffy**
Deputy Designated Safeguarding Lead (DDSL) - **Zoe Evans**
Designated people managing online presence - **Marketing Dept.**

Aims

The aims of our safety policy are:

- To protect all children and young people involved with our organisation and who make use of technology (such as mobile phones, consoles and the internet) while in our care.
- To provide staff and volunteers with policy and procedure information regarding online safety and inform them how to respond to incidents.
- To ensure our organisation is operating in line with our values and within the law regarding how we behave online.

Prevent Duty and Online Radicalisation

As part of our commitment to safeguarding and promoting the welfare of all individuals, EDT recognises its responsibilities under the Prevent Duty, as outlined in the Counter-Terrorism and Security Act 2015. We are committed to preventing the risk of radicalisation and extremism, including those risks that occur online.
The internet is a powerful tool for communication, learning, and engagement. However, it also presents significant safeguarding risks, including the possibility that children, young people, and vulnerable adults may be exposed to extremist content or influenced by radical ideologies.

Online Risks Include:

- Exposure to extremist propaganda, hate speech, and conspiracy theories through social media, forums, or video-sharing platforms.
- Recruitment and grooming by individuals or groups promoting extremist views.
- Access to materials that promote violence or justify terrorist acts.
- Echo chambers and algorithms that reinforce extreme ideologies without challenge.

Our Safeguarding Measures:

- We provide training for staff to recognise the signs of online radicalisation and understand how to respond to concerns in line with the Prevent Duty.
- Digital monitoring systems and acceptable use policies are in place to reduce access to harmful content.
- We educate service users, particularly those in vulnerable groups, about safe internet use, critical thinking, and how to report concerns.
- All concerns relating to extremism or radicalisation are referred appropriately, including to the Designated Safeguarding Lead (DSL) / Deputy Designated Safeguarding Lead (DDSL) and, where necessary, to external agencies such as Channel or Prevent coordinators. National Prevent Referral Form & Guidance

We acknowledge that individuals who are socially isolated, have unmet emotional needs, or experience discrimination or trauma may be more susceptible to online radicalisation. We strive to create a supportive environment where all users feel safe, included, and able to speak openly about any concerns.

Understanding the Online World

As part of using the internet and social media, our organisation will:

- Understand the safety aspects; including what is acceptable and unacceptable behaviour for staff and children – when using websites, social media, apps and other forms of digital communication.
- Be aware that it doesn't matter what device is being used for digital interaction, the same safety aspects apply whether it is a computer, mobile phone or game console.
- When using social media platforms (including Facebook, Twitter and Instagram), ensure that we adhere to relevant legislation and good practice guidelines.
- Regularly review existing safeguarding policies and procedures to ensure that online safeguarding issues are fully integrated including making sure concerns of abuse or disclosures that take place online are written into our reporting procedures.
- Provide training for the Marketing Dept as the people responsible for managing our organisation's online presence.

Managing our Online Presence

Our online presence through our website or social media platforms will adhere to the following guidelines:

- All social media accounts will be password protected and at least 3 members of staff will have access to each account password.
- The account will be monitored by the Marketing Dept.
- The Marketing Dept will remove inappropriate activity by children and staff explaining why, and informing anyone who may be affected (as well as parents of children involved).
- Account page and events will be set to private so that only invited members can see content.
- Identifying details such as a child's home address, school name, telephone should not be posted on social media platforms, internet, webinars, or any other online communication tools.
- Any posts or correspondence will be consistent with our organisation's aims.
- We will make sure children and young people are aware of who manages our social media accounts and who to contact if they have any concerns about the running of the account.
- Parents will be asked to give their approval for us to communicate with their children through social media or by other means of communication.
- Parents will need to give permission for photographs or videos of their child to be used on social media platforms.
- All accounts and email addresses will be appropriate and fit for purpose.

Use of Filtering and Monitoring Tools

In line with digital safeguarding best practices and guidance from the Department for Education, EDT recognises the importance of implementing appropriate filtering and monitoring systems to help protect users from harmful or inappropriate online content.

Where this organisation provides access to the internet or supplies digital devices to participants—whether on-site or for remote use—we will take reasonable steps to ensure that:

- Filtering software is in place to restrict access to content that is illegal, harmful, or not age-appropriate (e.g., content related to violence, extremism, pornography, or self-harm).
- Monitoring tools or systems are used, where appropriate, to detect online activity that may raise safeguarding concerns, including signs of online grooming, cyberbullying, or radicalisation.
- All filtering and monitoring practices are compliant with data protection laws and are used proportionately to safeguard users while respecting their privacy and dignity.

Our approach is regularly reviewed and balanced against the need to provide safe, open access to educational and support resources online. Where monitoring systems are in place, staff are trained to respond appropriately to any concerns raised through such tools.

We also provide clear guidelines and acceptable use agreements to participants regarding the safe and responsible use of devices and the internet. These outline expectations, prohibited behaviours, and how to report concerns or access support.

What we Expect of Staff and Volunteers

- Staff should be aware of this policy and behave in accordance with it.
- Staff should seek the advice of the DSL / DDSL if they have any concerns about the use of the internet or social media (also refer to EDT ICT policy).
- Staff should communicate any messages they wish to send out to children and young people to the DSL / DDSL.
- Staff should not friend or follow children or young people from personal accounts on social media or accept friend request from children or young persons. We recommend that all staff check their own social media for privacy settings to reduce the ability of young people finding personal accounts online.
- At least one other member of staff should be copied into any emails sent to children or young people, where appropriate, also include parent or guardian.
- Staff should avoid communicating with children and young people via email outside of normal office hours.
- Emails should be signed off in a professional manner, avoiding the use of emojis or symbols such as kisses (x).
- Any attachments should be professional, relevant and should have no personal information and use appropriate and age relevant language.
- Any disclosures of abuse reported through social media should be dealt with in the same way as face to-face disclosure according to our report procedures (please refer to EDT Safeguarding Policy).
- Staff should always use organisational accounts to communicate with children and young people via email or social media, **never personal accounts**.
- Staff should always use age-appropriate language in communications and make sure all their communications are restricted and relevant to the work of the project they are involved in.
- Staff should use an organisational mobile or tablet to communicate with young people, never personal devices.
- Staff should understand how different social media platforms work and what their age limits are. Use NSPCC Keeping Children Safe Online guides to find out about age restrictions on social networks, apps and games.

Using Mobile Phones or Other Digital Technology to Communicate

When using mobile phones (or other devices) to communicate by voice, video or text (including texting, email and instant messaging) we will take the follow precautions to ensure young people's safety:

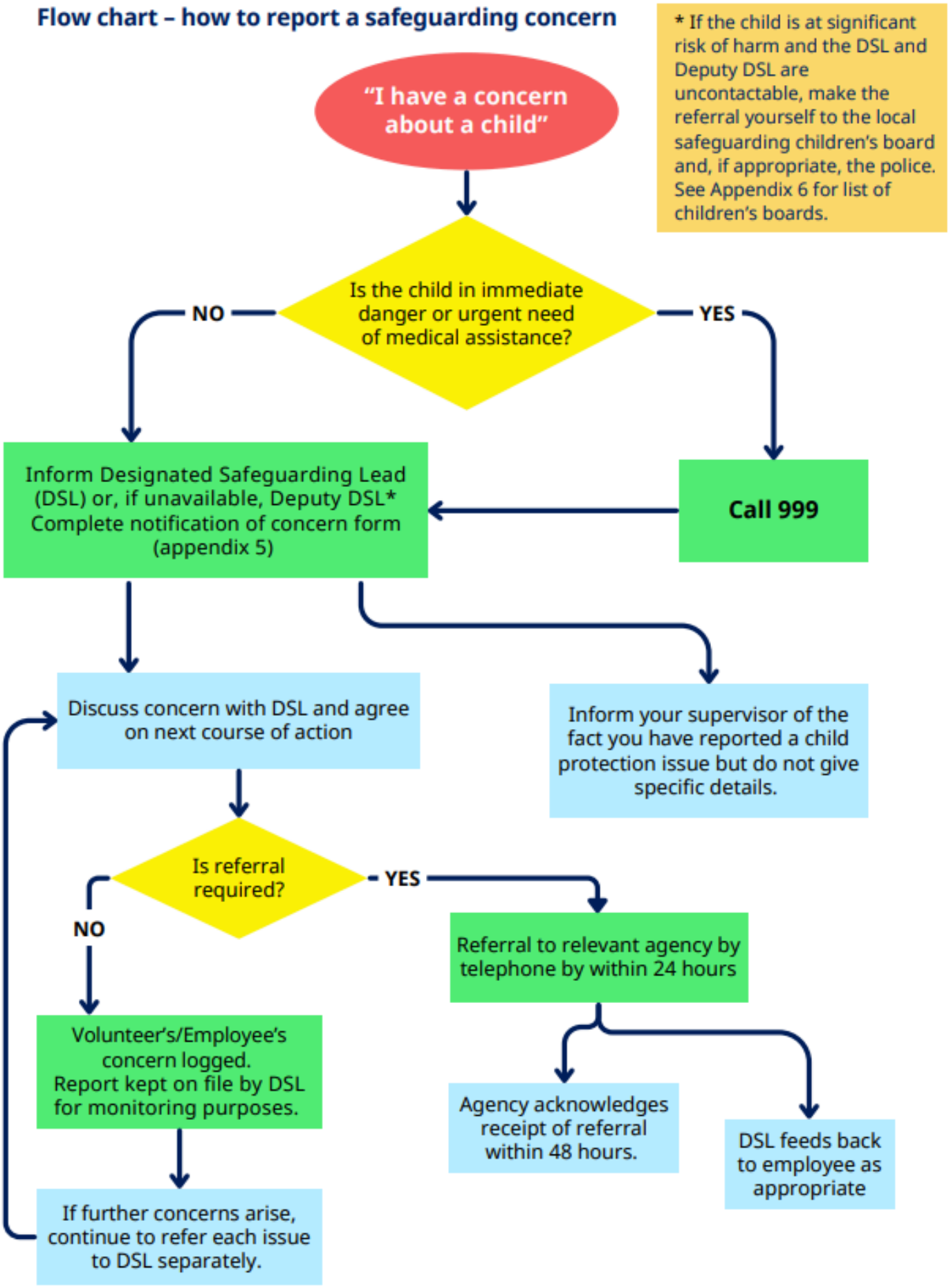
- Staff will avoid having children's or young people's personal mobile numbers and will instead seek contact through parents, guardians or teachers.
- We will seek parental permission when we need to contact children or young people directly, the purpose of contact will be clearly identified and agreed upon.
- Staff should have a separate phone from their personal one for any contact with parents or young people.
- Texts will be used for communicating information (always use inhouse texting facility) – such as reminding children or young people about upcoming events, which kit to bring or timings and not to engage in conversation.
- If a young person misinterprets such communication and tries to engage a staff member in conversation, the member of staff will take following steps:
    - End the conversation or stop replying
    - Suggest discussing the subject further at the next event or via responsible adult
    - If concerned about the child or young person, contact the DSL / DDSL.

Use of Other Digital Devices and Programmes

The principles in this policy apply no matter which current or future technology is used – including computers, laptops, tablets, web-enabled and smart TVs and whether an app, programme or website is used.
If any digital devices are used as part of activities with the organisation:

- We expect children and young people to adhere to the guidelines surrounding online use and behaviour set out in our on-line agreement.
- We will establish appropriate restrictions, more commonly known as 'Parental Controls' on any device provided to prevent misuse or harm.

Flow chart – how to report a safeguarding concern



* If the child is at significant risk of harm and the DSL and Deputy DSL are uncontactable, make the referral yourself to the local safeguarding children's board and, if appropriate, the police. See Appendix 6 for list of children's boards.

Reporting and Escalation Procedures (refer to EDT's Safeguarding Policy page 14)

Once any immediate action has been taken if appropriate, use the form in Appendix 6 in EDT's Safeguarding Policy document to record your concern or the disclosure.

All information about the suspected abuse or disclosure will be recorded as soon as possible after the event, in as much detail as possible and stating what actions, if any, were taken.