Digital Safeguarding Policy

DECEMBER 2023

Status	Final Version number: **1.0**
Approved by	Safeguarding Board Date: **14.2.2023**
Last updated	Date of this version: **Decembr 2023**
Review by	Date by when this must be reviewed and any updates made: **December 2025**
Owner	Policy owner name and role: **Volunteers and Safeguarding Manager**

Document control

Printed copies of this policy are up-to-date only on the date of printing from the intranet and must not be relied upon beyond that date.

The most up-to-date version of this policy can be found on the intranet.

Content

This document contains information as follows:

Policy statements	Must be followed	**Y**
Procedure	Must be followed	**N/A**
Guidance	Recommended practice that should be followed	**N/A**

Table of Contents

The Policy

This policy is part of the DofE's Safeguarding Framework to help us safeguard participants and others who come into contact with DofE through our activities. It should be read in conjunction with the DofE Safeguarding Policy.

It outlines the charity's policy, procedures and expected behaviours regarding interactions in the digital environment. It applies to all DofE staff (including temporary, freelance and casual staff) and volunteers who are engaged directly by the charity.

As part of our Safeguarding Framework, the policy sets out our expectations of anyone delivering DofE programmes or supporting DofE activities, such as Licensed Organisations (LOs), Approved Activity Providers (AAPs), or any other organisation or individual we may jointly work with.

Staff, volunteers and users in all organisations are also governed by safeguarding and other legislation and guidance provided by the relevant UK statutory bodies.

The DofE Safeguarding Procedures must be followed in the event of a safeguarding concern. It is understood that while the legal requirements apply to children, DofE applies the principles to all young people and adults at risk engaged with the DofE.

For full definitions of the terms used in this Policy, see the **Glossary of Terms**.

Policy statement

DofE's Safeguarding Principles:

1. The welfare of the child, young person or adult at risk is paramount.
2. All children, young people and adults regardless of age, race (including nationality, ethnic or national origin), sex, gender reassignment, disability, religion or belief, sexual orientation, marriage or civil partnership, pregnancy or maternity, have the right to equal protection from all types of harm or abuse.
3. Safeguarding must be person-centred, going beyond "protected characteristics" in order to recognise risks and barriers that some may experience (e.g., criminal record, immigration status or neurodivergence).
4. Safeguarding is everyone's responsibility, and everyone must play their full part in safeguarding children, young people and adults at risk.
5. All delivery partners of the DofE must adhere to the highest of safeguarding standards and practice and must adhere to DofE's Safeguarding Framework.
6. Children, young people, adults at risk and their families and carers should be seen as key partners in safeguarding and at the centre of all decision-making wherever possible.
7. Everyone must contribute to a safeguarding culture where people are listened to and allegations, concerns or views and wishes are taken seriously.

The purpose of this policy is to:

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

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

DofE is committed to the safeguarding and protection of all users of our digital services and social media channels, and we apply the same safeguarding principles to DofE's activities whether they are offline or online.

Context

The DofE is delivered across the UK under licence by nearly 5,000 organisations, known as 'Licensed Organisations' (LOs) who are licensed to deliver the DofE Programme and Approved Activity Providers (AAPs) who are licensed to deliver a section of the DofE Programme.

As part of the criteria for gaining a licence, each of these organisations must certify that they have their own satisfactory safeguarding arrangements in place. Safeguarding policies must address how participants are safeguarded in the digital space, including expected behaviours.

The LO or AAP's own safeguarding policy and procedures govern how it deals with all safeguarding incidents that occur in the context of its work. LOs and AAPs are required to report certain types of incidents to the DofE charity. (**dofe.org /run/runningprogrammes/incidents**).

The charity uses various digital platforms to communicate with a variety of audiences. We apply robust controls to eDofE, the DofE app, our emails, and our websites as we own and have control of these. However, we have limited control of platforms provided by other organisations and are thus subject to their restrictions and operating practices. Wherever possible, we try to mitigate these risks when using third party platforms.

Breach of the Policy

The DofE will take appropriate action in the event of breach of this policy.

Where DofE staff or volunteer conduct is found to contravene this policy, the DofE will deal with the matter in-line with the charity's relevant policies for managing staff and volunteers.

Where the breach occurs in a licensed organisation (LO or AAP), and the DofE becomes aware of the breach, we will deal with the matter in-line with the charity's relevant policies for managing licences.

In all cases, we will follow the DofE Safeguarding Policy and procedures and, where conduct is considered illegal or causes significant harm, the DofE will report the matter to the police and other relevant external agencies as appropriate.

The DofE is mindful that participants may behave in the digital space in a way that is not in-line with DofE Digital Behaviours (Appendix 1). In such cases, and in-line with our Safeguarding Principles, we will see the individual as someone who may be at risk and consider their safeguarding needs as well as those who may be affected, harmed or at risk from the behaviour. We will follow relevant UK law where we are required to report the matter to external agencies, such as the police.

Roles and responsibilities

The Designated Safeguarding Lead (**DSL**) has overall responsibility for ensuring that this policy is fit for purpose, understood by staff and volunteers, implemented effectively, and reviewed regularly.

All DofE staff and volunteers are responsible for making sure that they understand how to implement this policy in the context of their work and what procedures must be followed in the event of a digital safeguarding allegation being made.

The DSL (assisted by the Deputy Designated Safeguarding Lead, DDSL) will:

- Ensure that, 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.
- Ensure that staff and volunteers have an up-to-date awareness of the charity's digital Safeguarding Policy and that all staff and volunteers are aware of the procedures that need to be followed in the event of a digital safeguarding incident taking place.
- Keep up to date with developments in digital safety.

Staff and volunteers are responsible for ensuring that they:

- Have read and understood the DofE Safeguarding Policy, Code of Conduct and Digital Safeguarding Policy.
- Adhere to the behaviours and processes outlined in this policy and its appendices when carrying out their work or volunteering activity.
- Report any suspected misuse or abuse to the DSL/DDSL, in-line with the Safeguarding Procedures.
- Make sure that digital communications with children, young people and adults are appropriate and do not put people at risk.

Implementation and review

A copy of this policy document will be made available to all new DofE staff and, volunteers as part of their induction and its provisions will be covered in core safeguarding training.

All staff and volunteers must sign a statement that they have received, read and understood this policy and this will be held on central record. The Director of People and Culture is responsible for ensuring that a process is in place to facilitate this.

The content of this policy will be subject to a regular review cycle where recommendations may be made and monitored annually to ensure the effective implementation of this policy.

Procedures for DofE staff and volunteers

Reporting

Unacceptable conduct in the digital environment (e.g., defamatory, discriminatory, offensive, bullying, harassing behaviour, accessing inappropriate pornographic material or a breach of data protection, confidentiality, copyright) will be taken extremely seriously by the DofE.

DofE staff and volunteers must report such incidents as soon as possible to the safeguarding team by emailing **safeguarding@dofe.org**.

Licensed Organisations should follow their safeguarding policy and requirements set down in the License.

In line with our Safeguarding Policy and Procedures, participants, members of the public, staff and volunteers of LOs and AAPs may also report digital safeguarding concerns to the DofE safeguarding team by emailing **safeguarding@dofe.org**

Use of social media

DofE staff and volunteers must not use DofE social media channels to infringe on the rights and privacy of others, or make inappropriate comments or judgments. DofE social media accounts must not be used for personal gain.

Staff and volunteers must ensure that confidentiality around information relating to participants, volunteers, and staff, is maintained on DofE social media and must relinquish admin rights to any DofE social media accounts before they leave the employment of, or cease to volunteer for, the DofE.

It is the responsibility of the relevant line manager to ensure this happens.

Staff and volunteers using DofE social media accounts must:

- Know the contents of this policy and ensure that any use of social media is carried out in-line with this and other relevant policies or guidelines.
- Attend any training that is deemed necessary for safely using social media platforms.
- Regularly monitor, update, and manage content they have posted, or has been replied to, via DofE accounts to ensure appropriate usage.
- Respond to complaints made via social media without delay during office hours and as soon as possible outside of office hours, even if the response is only to acknowledge, and should be forwarded to **complaints@dofe.org** or logged on Zendesk.
- Follow the DofE Media Policy: if a journalist makes contact about content on social media, do not respond directly and refer to the Senior Media and Communications Manager.

Managing misuse:

- When acting on behalf of the DofE, handle offensive comments swiftly and with sensitivity.
- If a conversation becomes offensive or unacceptable, DofE users should block, report, or delete other users or their comments/posts.
- If the content is deemed as potentially illegal – child sexual abuse content or extremism – then the appropriate reporting channels must be followed.

If you feel that you or someone else is subject to abuse by DofE staff or volunteers through use of a social networking site, then this action must be reported to the DSL or DDSL without delay.

The DofE does not monitor staff or volunteer's personal social media accounts on a regular basis, but expects that all its staff and volunteers will conduct themselves in-line with the Code of Conduct both online and offline. Staff and volunteers using social media accounts which are not part of the charity's official communications mechanisms, but which state that the individual operating the account is linked to the DofE must use the following disclaimer:

(Job title) at The DofE. All views, posts and opinions shared are my own.

Further guidance can be found on the use of personal accounts in the Social Media Playbook.

Use of images

Many DofE activities involve recording images. These images may be created for publicity purposes, to celebrate achievement or to provide records of evidence of the activity.

Whilst images are nearly always used for very positive purposes, adults need to be aware of the potential for these to be misused or manipulated for pornographic or 'grooming' purposes. Particular thought needs to be given when images are taken of young children or young people or adults at risk who may be unable to question why or how the activities are taking place.

Staff and volunteers must not take photographs or videos of DofE participants who are under 18 on personal devices e.g., mobile phones, tablets etc. If images are required for publicity or reporting purposes, they should be sourced via the LO or through the DofE Communications Team who will gain the appropriate release permission via the model/case study release forms.

Staff may post content:

- Where the appropriate permission via model/case study release forms have been given to DofE. This can include re-posting DofE social media content, provided the above permission protocols have been followed when obtaining the image.

- From social media accounts owned by third parties such as LOs or other reputable authors e.g., local authorities, other national youth bodies etc. This is because consent will have been obtained by the LO in-line with their licensing conditions or by other organisations in-line with their own policies. If in doubt, you should seek confirmation from that third party before posting.

In all cases, staff should consider the safety and safeguarding of the individual/s and whether there are any known factors which may place the individual/s at risk if content relating to them is shared. Staff should be mindful that, even though consent has been obtained, circumstances may change or the participant, their parent or carer may not have considered the risks. Always seek advice from the DSL if you are in doubt.

When using images for any publicity purposes, first names only should be used in any captions or editorial. LO name and county/hometown can be added but only if the specifics are important for context.

Where surnames are required e.g., press articles, permission must be sought from the participant/Award holder or parent/carer/guardian, (under 18s) using the communications teams' case study release forms: **DofE - Individuals consent form_2023.docx**

Communication between staff, volunteers and participants

Communication between staff or volunteers and participants under 18 must only take place using DofE-approved methods. This includes through eDofE, an official DofE email address, Zendesk, DofE-owned social media accounts or a DofE contract phone. The eDofE messaging system should be the preferred method of communication, wherever possible. Where a different method is used such as phone, text or suitable messaging app (e.g., Slack), it must be used in line with this policy.

Staff may use text messaging or calls to communicate with participants, provided:

- They are permitted to do so as part of **performing** their role and responsibilities (e.g., responsible for participants attending an event or activity).
- They have consent from the participant (over 18) or parents/carers (under 18) to do so.
- The contact is for the purpose of performing their role and responsibilities and not for social contact.
- The phone used is a DofE-issued contract mobile phone or DofE landline.
- Participants and parents/carers receive information about when and how contact will be made and have the choice of how they prefer to be contacted.
- The above information is clear, and a DofE landline or mobile phone must always be used to ensure safeguarding, transparency, and accountability.

- All calls should be logged on the charity's CRM system.
- It is a case of an emergency or other unplanned circumstance that could not reasonably be anticipated.

Staff must ensure that a work mobile phone is turned off at the end of the working period.

Voicemail messages must be kept for a period of no less than three months to enable access if required.

Where an adult has care and support needs, direct contact may not be appropriate due to communication, learning or other additional needs. You should check with the participant and parent/carer (where appropriate). If in doubt, seek advice from the DSL/DDSL.

When using digital communications, staff and volunteers must:

- Only make contact with participants for professional reasons.
- Not share any personal information with participants e.g., must not give their personal contact details to participants including private email, home or mobile telephone numbers.
- Not request or respond to requests for any personal information (e.g., home life, relationships etc) from the participants, other than that which might be appropriate as part of their professional role.
- Be aware of and use the appropriate reporting routes available to them if they suspect any of their personal details have been compromised.
- Ensure that all communications are transparent and open to scrutiny.
- Follow up calls (whether incoming or outgoing) with an email, to provide an audit trail. Where this is not appropriate (e.g., a call to check whereabouts due to late arrival), a short note logging the call/s is sufficient. This should be kept on the project/planning file.
- Only make direct contact in exceptional circumstances.
- Be careful in their communications with participants so as to avoid any possible misinterpretation.

eDofE

eDofE is a proprietary system, developed and maintained by the charity. Participants use it to record progress on their award programme, adults record their DofE training and affiliations to LOs/AAPs and it is an important tool for DofE staff to use to manage the DofE network.

Messaging functionality exists within eDofE which allows different users to contact each other within their hierarchy. All messages are monitored, passing through an automated system which analyses them for different words or phrases and any activity of a nature which raises concern is followed up by the DSL/DDSL as appropriate.

Staff and volunteers must:

- Use the eDofE messaging function as their primary method of communicating with young people, where possible.
- Report any images or other content within eDofE that is of an inappropriate nature to the DSL/DDSL.

Video conferencing and virtual classroom tools

Calls using a webcam can be used for one-to-one communications and group conference calls and are considered appropriate if a project team or other group needs to discuss plans for events and activities.

When staff or volunteers are communicating with those under 18, who are not employed by the DofE, they must choose a platform that:

- Enables individual users to join without setting up an account.
- As far as possible avoids sharing an individual users' phone or email address with other users. This may be achieved by using the bcc function on email when sending out the link for the online meeting and platforms such as Zoom or Adobe Connect.
- Is free from marketing and advertising.
- Is flexible, enabling individual users to turn their microphones and webcams on and off.
- Uses a secure and encrypted connection (if unsure check with DofE's IT directorate).
- Is suitable for the target age group and enables their participation.
- Logs sessions and operates in office hours. When operating outside of normal office hours, the relevant line manager will be informed as part of the risk assessment and planning process.

Two adults must be present in all virtual group meetings with participants, and it is good practice to set a start and finish time.

At no point should a participant find themselves in one-on-one conversation with any single member of staff, volunteer or other adult. Other participants or DofE staff and volunteers must always be present.

Breakout room group sessions must contain at least three participants and should be checked in on by at least one member of staff or volunteer during the breakout period.

Staff and volunteers must obtain parental consent before webcams are used with young people outside of the Licensed Organisation's usual environment (e.g., the school classroom, youth charity meeting place or environments where the LO would normally meet or operate).

Before seeking such consent, full details of why a webcam is to be used should be provided. This should also include information on the use of images, who is to be given authority to view them, and the security measures which will be implemented to prevent unauthorised access.

It is recommended that meetings with young people under 18 are not recorded, however if recording takes place, children, young people, parents and carers, Leaders and their Managers should be consulted. Written consent should be obtained from all parents and carers. Consideration must be given to informed consent in relation to adults with care and support needs.

Any recordings should be retained for a limited time period only and for no longer than is necessary. This will generally be a maximum of no more than 30 days from the recording taking place unless stated otherwise (e.g., recordings of training webinars).

It is the responsibility of the staff member who initiated any recording to ensure that all copies are destroyed after the stated date.

Chat functions and direct messaging

Staff and volunteers must use the messaging function in eDofE whenever possible to communicate with participants.

The use of direct messaging using social apps and chat functions may be used where it is necessary, and the application used can provide an audit trail (See Communication between Staff, Volunteers and Participants section). This will usually be for one of DofE's streams of planned direct work e.g., Youth Ambassador Programme. At present, DofE uses Slack for communication with participants in some projects as it meets these requirements.

Where an adult has care and support needs, direct contact may not be appropriate due to communication, learning or other additional needs. You should check with the participant and parent/carer (where appropriate). If in doubt, seek advice from the DSL/DDSL.

Appendices

Appendix 1: Digital behaviour

Alongside the DofE Code of Conduct, which all DofE staff and volunteers must follow, the below describes standards of behaviour expected from everyone engaged in DofE activity within digital settings:

The DofE expects that DofE staff, volunteers and others facilitating the DofE programme (including temporary, freelance and casual staff) will:

- Be a good role model at all times.
- Ensure that all young people and adults at risk are safeguarded by following safeguarding policy and procedures.
- Immediately tell the police if you think a crime is being committed or that a young person or adult at risk is in immediate, serious risk of harm.
- Undertake regular safeguarding training appropriate to your role.
- Not share personal digital information (e.g., social networking profiles) with the children and young people that you meet through your role with DofE.
- Abide by the organisation's data protection policies.
- Not deliberately bypass any systems designed to protect your organisation or young people.

In addition, DofE staff and volunteers will:

- Report any safeguarding concerns, allegations or disclosures as soon as possible (always within 24 hours) to **safeguarding@dofe.org**
- Not attempt to install programmes of any type on the devices belonging to the charity without permission or authorisation from the DofE IT Directorate.
- Not access anything illegal, harmful or inappropriate from a DofE device.
- Ensure that your digital activity does not bring the DofE into disrepute.

It is good practice to think carefully about how any digital communication might appear to a third party. Compared with a conversation in the real world, technology increases the potential for messages to be seen out of context, to be misinterpreted or forwarded to others.

The use of sarcasm and innuendo are not appropriate, and individuals must take care to avoid "banter" or other types of comments which could be misinterpreted when they are communicating with participants in particular.

It is DofE's expectations that everyone will:

- Treat each other with dignity and respect in line with the DofE's values.
- Respect one another's privacy.
- Be responsible and accountable.
- Not share personal passwords or those of other users.
- Not download anything that you do not have the right to use.

Appendix 2: Related policies, procedures, and documents

- Incident Reporting for Licensed Organisations and Approved Activity Providers

DofE Safeguarding Steering Board Terms of Reference

- Safeguarding Policy **DofE, Safeguarding Policy**
- Safeguarding Procedures **Safeguarding Procedures (including Child Protection)**
- Low-Level Concerns Policy **Low-Level Concerns Policy - April 2023.pdf**
- Recruitment & Selection Policy

HR Policies

- **Volunteer Policies**
- **Licensing Policy**
- **Data Protection Policy**
- **Equality, Diversity and Inclusion Policy**
- **Complaints Policy**
- **Speak up (whistleblowing) policy**
- **Incident Management Guidance**

Social Media Playbook:
Internal - Social_Media_Playbook(1).pdf - All Documents (sharepoint.com)

Appendix 3: Glossary

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 (usually staff or volunteers) 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 the Code of Conduct and falls short of standards expected by DofE.

Approved Activity Provider (AAP): organisations whose opportunities have been approved by the DofE as meeting its sectional conditions and can count towards the achievement of a DofE Award. AAPs may have charitable or commercial status.

Child or young person: anyone under the age of 18 years.

Child protection: is part of the safeguarding process. It focuses on protecting individual children identified as suffering or likely to suffer significant harm. This is the threshold at which local authority intervention is considered necessary in order to protect the child.

Company phone: a mobile phone that is on contract solely to the DofE and is issued by the charity to an employee for business use. It does not include any phone that is on a personal contract irrespective if the DofE contributes to the monthly payments.

Designated Safeguarding Lead (DSL): The person who leads and has accountability for safeguarding and child protection and ensures that the organisation is following the appropriate safeguarding policies and practices. This person is accountable to the organisation and to the DofE Board of Trustees. They are supported by a Deputy Safeguarding Lead (DDSL).

Disclosure: is where someone tells another (e.g., staff or volunteer) information that describes or indicates abuse or harm.

Emotional (or psychological) abuse: continual emotional mistreatment including intimidation or bullying, humiliation, threats, isolation.

Financial (or material) abuse: a breach of trust which involves theft of money or possessions such as bullying, misuse of money or preventing access to it; scamming or fraud.

Grooming: when someone builds a relationship, trust and emotional connection with a child or young person or adult so they can manipulate, exploit and abuse.

Incident: is any event that occurs which involves and/or impacts on the safety of children or adults. It may not be a safeguarding concern initially (although it may become a safeguarding matter, on further investigation). It may relate to health and safety practices, participant behaviour, a complaint or feedback. However, it must be reported and investigated in order to safeguard children and adults and prevent escalation.

LADO (Local Authority Designated Officer): Person who: has oversight of allegations about practitioners who pose a risk to children; gives advice to agencies; ensures appropriate action taken and information is shared appropriately with other agencies. In some local authorities the same officer or similar appointment will deal with concerns about practitioners who pose a risk of harm to adults at risk. They may also be referred to as the DASM (Designated Adult Safeguarding Manager). For the purpose of this policy, LADO will refer to the designated local authority lead for both adults and children in England and Wales or the equivalent person in Scotland and N Ireland.

Leader: A person supporting a child or young person whilst they are participating in their DofE programme. A participant undertaking a leadership role as part of their own programme would also be considered a Leader.

Licensed Organisation (LO): organisations which have been awarded a licence by DofE to deliver DofE activities. This may include, for example, local authorities, schools, charities and private companies.

Mental Capacity: The ability to consider relevant information, make and communicate a decision.

Neglect: is the ongoing failure to meet the needs of a child or adult at risk. This may include leaving them hungry, dirty, no access to shelter; not attending to medical or health needs.

Parental consent: Parental consent must be in a written format, either using the DofE Comms team's media consent form, the LO's media consent form which explicitly gives permission for third party usage or an email/text from the parent/carer/guardian that states that images of their young person can be used by the DofE on social media/publications.

Participants: anyone aged 13-24 who is undertaking a DofE Award through a licensed organisation or DofE Direct; taking part in DofE programmes such as Young Leaders and Youth Ambassadors or representing DofE as an ambassador.

Personal details: This may include but is not exclusive to; home address, home phone number, non-DofE personal email, religious or philosophical beliefs, political beliefs, sex life or sexual orientation, marital status, mental health.

Personal phone: This is a mobile phone that is on a personal contract solely to an individual and is not issued by the DofE irrespective whether the DofE contributes to the monthly payments.

Physical Abuse: hurting or harming a child or adult at risk intentionally including hitting, slapping, rough handling, physical punishments and restraints.

Policy: A statement of principle, action or plan adopted by an organisation.

Procedure: A method of carrying out a policy.

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.

Safeguarding: is the action that is taken to promote the welfare of children and at risk adults 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 is protecting their rights to live in safety, free from abuse and neglect.

Sexual Abuse: forcing or tricking someone into sexual activities including rape, inappropriate touching, indecent exposure, forcing of creating or watching sexual photography.

Staff: anyone employed by DofE including agency staff, those on secondment or placement and contractors.

Volunteer: anyone carrying out a volunteer role for DofE in which they are managed by and/or it has been agreed in writing that they are directly responsible and accountable to DofE whilst carrying out their role. This includes but is not limited to trustees, volunteers for programmes such as DofE Direct and Young Ambassador and others acting as ambassadors for DofE from time to time. The term excludes those persons acting in a volunteer capacity for LOs or AAPs or any organisation other than DofE.

Working period: period in which an individual is officially active in their DofE role. This would usually be office hours but may be during the weekend or evening when delivering activities on behalf of the DofE as per contract.