Diocese of Bristol

Digital Safeguarding Policy

Issue date: Oct 2023
Last review date: Oct 2023
Next review date: Oct 2026

Purpose

The Diocesan Board of Finance (DBF) works in the digital space, capturing and communicating content online about young people and their projects, across the Diocese of Bristol (DOB). DBF uses digital technologies to champion young people and connect them with the information, people, and resources they need to succeed.

We recognise however, that there are as many Safeguarding risks associated with digital engagement, as with physical engagement. We also recognise that our digital network comprises of people from all backgrounds, including vulnerable adults and children, who may need support.

This Digital Safeguarding Policy ('Digital Safeguarding Policy' or 'Digital Policy') has been developed to address these risks and ensure that we are keeping the people we work with safe from harm.

This Digital Policy should be read in conjunction with the Safeguarding Policy. **Should you wish to report a safeguarding concern, please contact us directly here.**

Scope

While everyone, without exception, has the right to protection from abuse, regardless of factors such as age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief or sex or sexual orientation, the focus of this policy is to protect children, young people, and vulnerable adults from harm. These categories are not mutually exclusive.

Children

DBF defines children as anyone that has not yet reached their 18th birthday. This is in line with the United Nations Convention on the Rights of the Child and civil legislation in England and Wales. The fact that a child has reached 16 years of age, is living independently or is in further education, is a member of the armed forces, is in hospital or in custody in the secure estate, does not change their status or entitlements to services or protection. DOB works directly with children, through our work in schools, parishes, and other educational and pastoral environments.

Young People

DOB works with young people aged 18 - 35 years of age. Young people are considered by DBF to be any individuals who are within this age range.

Vulnerable Adult (or Adult at Risk)

An adult is vulnerable if they require protection and is, or may be, in need of protection by reason of age, illness, mental or other disability, and/or who

lives with economic dependence, a conflict environment or cultural constraints. We recognise that vulnerability can be transient, due to changes in environment, capacity or resources. Therefore, we recognise that a person who was not before, may become vulnerable, that it is possible for vulnerability to be just temporary state, or be more pervasive.

DOB Representatives

- Clergy
- Ministers
- Board members
- Staff members
- Volunteers
- Consultants
- Contractors
- Partners

DOB Visitors

Those who visit DBF or individuals across DOB, in a professional or support-seeking capacity, with DBF's knowledge and consent (including but not limited to journalists or congregation members).

General Principles

DBF considers that, without exception, it is unacceptable for any person, of any age, to experience any kind of abuse or exploitation, and that safeguarding children, young people and vulnerable adults and protecting them from harm is everyone's responsibility.

We are committed to:

- Providing our representatives, visitors and young people with information, advice, and procedures on using digital platforms and social media and staying safe online;
- Taking appropriate steps to safeguard young people online, including children and those adults deemed at risk;
- Developing and reviewing our policy and protocols regularly.

We expect every person and organisation we engage with to commit to and adopt these principles and commitments as their own.

Digital Risk

DBF aims, always, to minimise the risk of a Digital Safeguarding incident occurring because of its engagement with children, young people, and vulnerable adults.

- There are several key forms of Digital Risk:
- **Conduct:** Risks include the behaviour of the aggressor (i.e. bullying/harassment) and the behaviour of the victim (sharing personal information);
- **Content:** Risks include exposure to age or culturally inappropriate content and unreliable information and extremist material.
- **Contact:** Risks occur when the digital and physical worlds are drawn together, through bullying/trolling/online grooming etc.
- **Scamming to obtain financial reward:** Risks include hidden costs, for example in apps, 'phishing' or other methods of identity theft.

Diocese of Bristol

What might constitute a digital safeguarding incident?

Safeguarding incidents include concerns or allegations from an individual child, young person or vulnerable adult and can be made against DOB Representatives or Visitors. They could, for example, include the following behaviour:

- Bullying/trolling by peers and people they consider 'friends';
- Threats of harm (physical, psychological);
- Posting personal information that can identify and locate a child, young person or vulnerable adult offline;
- Sexual grooming, luring, exploitation, and abuse through contact with strangers;
- Harassment
- Impersonation/ misrepresentation of any kind;
- Exposure to inappropriate content, including indecent images of children/ child abuse material / sexual content, profanity, extremist material; spam, advertising, URLs that lead to material not authorised/endorsed by DBF;
- Involvement in making or distributing illegal or inappropriate content;
- Theft of personal information/identity theft;
- Exposure to information and interaction with others who encourage self-harm/suicide;
- Exposure to racist or hate material;
- Encouragement of violent behaviour and the recording of an assault for the purpose of widely sharing the recording;
- Promoting violence and acts of terrorism;
- Glorifying activities such as drug taking or excessive drinking;
- Physical harm to people in making video content, such as enacting and imitating stunts and risk-taking activities;
- Leaving and running away from home because of contacts made online;
- Defamation and/or breach of copyright.

Where might digital safeguarding incidents take place?

A Digital Safeguarding Incident can occur anywhere across an organisation's digital footprint. A digital footprint is a unique set of digital activities, actions, and communications that can identify an organisation online.

A digital footprint of a Diocese can be extremely broad and - because it comprises everything that individuals working for parishes have said, as well as those working for DBF, and everything others have said about the organisation - not all of a digital footprint is under the control/influence of the organisation itself. A digital footprint can include, but is not limited to, content that can be found via:

- Organic search;
- Directories, event platforms and review sites;
- Emails sent;
- Social media/social sharing;

- Influencers & affiliates;
- Blogs;
- Marketplaces;
- Brand Partnerships;
- PR.

In addition to the 'official' digital footprint of an organisation – that is, content created at the direction, or with the endorsement of the organisation, there exists significant potential for a large 'unofficial' digital footprint to exist.

This 'unofficial' footprint includes genuine user-generated content (such as reviews or posts in networking group) and illegitimate content. **Unofficial content, in whatever form, poses significant Digital Safeguarding risks.**

The greatest Digital Safeguarding risk is posed by social media. Social media refers to digital platforms that provide such services as blogs, discussion forums and instant messaging. Social media includes, but is not limited to:

- Social networking sites e.g. Facebook
- Micro-blogging services e.g. Twitter
- Video-sharing services e.g. YouTube
- Photo-sharing services e.g. Instagram

Social media platforms often incorporate more than one of the features listed alongside their primary services.

Examples of popular social media sites include, but are not limited to: LinkedIn, Twitter, Facebook, YouTube, Instagram, Snapchat, Flickr, TikTok, Yammer, Yahoo/MSN messenger, Wikis and blogs, Weibo, WeChat and WhatsApp.

Responsibilities

Diocesan Secretary

The Diocesan Secretary has overarching responsibility for ensuring the content of this policy is applied consistently and fairly across the DBF. Within the Diocesan Office, the Diocesan Secretary delegates to the Staff Leadership Team the responsibility to ensure that the DBF adheres to Digital Safeguarding Guidelines when communicating online.

Director of External Relations

The Director of External Relations is responsible for:

ensuring this policy is disseminated effectively to teams and that all teams understand and adhere to it.

leading the External Relations Team, who take responsibility for monitoring the DBF digital footprint.

Safeguarding Team

The Safeguarding Team holds responsibility for investigating Safeguarding issues, as reported to them by the Designated Digital Safeguarding Officer (DDSO). Where it is deemed necessary, they are responsible for investigating breaches of the policy from team members.

Team members

Team members are responsible for ensuring personal views or actions on

personal and professional online accounts do not breach the principles of the Digital Safeguarding Policy.

Procedure

Digital Monitoring

While we do not actively moderate user content, we will monitor our digital footprint and will report or remove and user content, which could be deemed a digital risk.

Our known digital footprint is monitored by the DDSO, using Google Alerts, and other monitoring and tracking tools. The DDSO will seek advice from the DBF Safeguarding team, where Safeguarding concerns arise.

The DDSO will have the authority to:

- remove and log ANY content of any nature that is deemed inappropriate;
- report the user and the content to the relevant digital / social media channel;
- escalate to the DBF Safeguarding team, where necessary.

The DDSO will act without waiting for a second opinion from anyone, if they feel the situation merits such action. DBF's policy in this regard is to act first to remove/report inappropriate content.

Data Protection

DBF's Privacy Policy outlines how we protect the privacy of others and adhere to data protection laws in relation to any personally identifiable information (PII) that is collected, stored, used, or shared.

We recognise that additional measures may, from time to time, need to be taken regarding Data Protection in a Safeguarding context.

In situations where children young people or adults deemed at risk may need extra protection, DBF will seek to protect identities and moderate content accordingly, with only first names and non-identifiable locations used.

In extremely sensitive cases, a first name can be changed, or a pseudonym used, to protect an individual's identity, and will be footnoted with the following:
"Names have been changed in order to protect the identities of those involved."

Guidelines for online conduct and safeguarding are provided to Clergy via our Clergy Handbook.

Informed Consent

DBF will only publish stories and images, still or moving, where it is satisfied that informed written consent has been received, from the adult featured or the person's parent/guardian as appropriate. This consent will be stored alongside the data provided, as either a personal consent form or carer consent form, as appropriate.

DBF will ensure individuals can see how content featuring them is being used and shared, disclose any potential risks, and ensure individuals

are aware of their rights so that informed consent can be given.

Third parties supplying content to DBF will be required to demonstrate that they have acquired written consent from those featured.

Where a project has a focus on children under 12, careful consideration will be given to the most appropriate format to publish online.

Trust

Trusted Content

DBF endeavours to share content that does not mislead its audience and does not seek to control the conversation. Content will not click through to unexpected destinations and will only link out to trusted and relevant third parties.

Please refer to our Terms and Conditions to understand our general approach to user content and to access the code of conduct that we expect all users of our digital footprint to abide by.

Trusted Communications

When working with children, young people and vulnerable adults connected with DBF, only official communication channels will be used. Diocese of Bristol Representatives and Visitors should only use official email, social media accounts and networking groups. If a Representative or Visitor cannot use an official account themselves, they must seek support from someone that can.

Personal email, social networking accounts, private networking groups or other means of unofficial communication are an inappropriate communication method.

Messages for children should be passed through parents and guardians, or through their school, with their parents/guardians informed. **Messages should never be passed directly to children.**

Official Diocese of Bristol Communication Channels

The Diocese of Bristol website domain is: bristol.anglican.org.

All official emails will originate from bristoldiocese.org domain. This means that every official DOB/DBF email account will contain a person's first name and last name, followed by @bristoldiocese.org. No other domain will be used.

DOB's official social media presence includes:

- Twitter: @diobrizzle
- Instagram: @dioceseofbristol
- Facebook: @Diocese.of.Bristol
- LinkedIn: diocese-of-bristol
- TikTok: @dioceseofbristol

The DDSO must be part of a networking group for it to be considered an official networking group.

Any new networking platform, networked group or social media account should only be created with the approval of the Director of External

Relations or Deputy Director of External Relations.

If you discover an email, social media account, or networking group, alleging to represent DOB that is not listed in this policy, please get in touch.

Account Security

Our email service is provided by the Church of England IT department via Microsoft Outlook. Administrator access to this service, which is required to change our domain or to add new users, is available only to the Church of England IT department.

The email addresses associated with our online accounts will always use "bristoldiocese.org" emails, or in the case of Google products, the bristoldiocese@gmail.com email. Passwords for these accounts are held centrally on the LastPass database, by the Deputy Director of External Relations. **Passwords are not stored anywhere else.**

The changing of usernames/handles, email addresses and passwords for these accounts is prohibited unless the new details are stored within the LastPass account.
This is to ensure that every account:

- is consistent with the advice provided in this policy;
- aligns with DBF's Communications Strategy;
- aligns with DBF's Brand Strategy and guidelines.

DBF takes all breaches of security seriously and will act to improve account security at every opportunity, considering all disciplinary options available to it in response to a security breach. This includes anything from suspension of access to termination of relationship with any Representative or Visitor found to be in breach of this Digital Safeguarding Policy.

Breach of this policy

We will monitor our digital footprint across our corporate online accounts. We may have to take disciplinary action leading up to and including dismissal if team members do not follow this policy's guidelines.