

Church For Everyone – Autistic Community Safeguarding and GDPR Approach

Baselined Document

April 2025

Version: 1.0
Issued: 02/04/2025
Author: Stewart Rapley

Document Control

[illegible]

CFE-A: Safeguarding & GDPR Approach

Introduction

We do not constitute an 'organisation' for the purposes of UK Safeguarding Regulations and General Data Protection Regulations (GDPR).

We have no formal requirement for compliance with these regulations (drafting and maintaining policies, providing training etc.). Many of these sound good in themselves but can generate significant volumes of bureaucracy!

We operate no 'membership' – participants are free to come and go as they please. We are also not seeking to operate as a 'pastoral group'; there is no implied 'formal responsibility of care' from one to another.

Many of us will be subject to the policies and training requirements of our local, regional or national churches – this is in connection with our engagement with these churches.

We do, however, wish to comply with the spirit of these requirements as they represent values of kindness and respect that we would want to uphold from a Christian perspective anyway.

This document proposes an approach that, I hope, supports the principles and spirit within what is an appropriate level of administration.

CFE-A: Safeguarding & GDPR Approach

Safeguarding 1

The Care Act 2014 (url below) applies to England and Wales – similar provisions are covered in a range of Scottish legislation (e.g. Public Bodies (Joint Working) (Scotland) Act 2014).

The Care Act identifies 6 safeguarding principles (url below):

1. Empowerment: “giving individuals as much freedom and power over decisions made about themselves as is reasonably possible.”
2. Prevention: “It is far better to take steps to prevent safeguarding issues from occurring rather than dealing with the situation when they do.”
3. Protection: “the core act of giving vulnerable people care and support when they need it.”
4. Proportionality: “it’s important that every case is dealt with individually and with all the facts taken into account, without excessive intrusion.”
5. Partnerships: “Safeguarding should be a communal process rather than the sole responsibility of certain individuals.”
6. Accountability: “while named [individuals] are most responsible for safeguarding, it’s up to everyone to do their part.”

<https://www.legislation.gov.uk/ukpga/2014/23/contents/enacted>

[https://www.virtual-college.co.uk/resources/what-are-the-6-principles-of-](https://www.virtual-college.co.uk/resources/what-are-the-6-principles-of-safeguarding#:~:text=What%20are%20the%20Principles%20of,%2C%20proportionality%2C%20partnerships%20and%20accountability.)

[safeguarding#:~:text=What%20are%20the%20Principles%20of,%2C%20proportionality%2C%20partnerships%20and%20accountability.](https://www.virtual-college.co.uk/resources/what-are-the-6-principles-of-safeguarding#:~:text=What%20are%20the%20Principles%20of,%2C%20proportionality%2C%20partnerships%20and%20accountability.)

CFE-A: Safeguarding & GDPR Approach

Safeguarding 2

It is proposed that we operate as follows:

1. We nominate one individual within the group as an informal 'Designated Safeguarding Person' DSP – to act as a point of contact for any concerns that may need to be raised.
2. This DSP maintains contact details that are available to all participants in the group (described as 'open' on GDPR slides).
3. For each of the 6 principles, we develop a short statement of 'what this means' in our context.
4. We make individuals aware of safeguarding training that is available, accessible and relevant, and also further information on Safeguarding.
5. Any concern about the DSP should be raised with the group co-ordinator.

Sources of available Safeguarding Training:

tbc

Church-specific information on Safeguarding:

St James & Emmanuel: <https://stjamesandemmanuel.org/safeguarding-children-and-vulnerable-adults/>

Other: tbc.

CFE-A: Safeguarding & GDPR Approach

GDPR 1

The 7 principles of GDPR are drawn from a range of sources, but significantly Convention 108, issued by the Council of Europe. This dates from 1981 (url below) but has been regularly updated since.

The 7 GDPR principles (url below):

1. Lawfulness, fairness and transparency: data must be processed in an open, legal, and fair way.
2. Purpose limitation: data can used only for the purpose for which it is given.
3. Data minimisation: only that data which is required for the intended purpose should be obtained or held.
4. Accuracy: personal data should be maintained as up to date.
5. Storage limitation: data should only be held for the specified time.
6. Integrity and confidentiality: data needs to be protected from accidental change, loss, damage or destruction.
7. Accountability: we must be able to demonstrate how we are handling held data.

<https://www.coe.int/en/web/data-protection/convention108-and-protocol>

<https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/>

CFE-A: Safeguarding & GDPR Approach

GDPR 2

It is proposed that we operate as follows:

1. In our context we are primarily concerned about the holding of email addresses.
2. As part of an annual 'start-up' in January, I will send each person on the current mailing list a personal email indicating their current preference for **open** (can be used in open communication with the group – visible to everyone), or **closed** (can only be used in bcc fields in emails or 'withheld' in attendee lists for meeting invites. This email will request notification of any change between these options, and will include an option to 'remove email address from list' in acknowledgement that sometimes people move on and no longer wish to receive communication from or about the group.
3. Email addresses will then be used according to the open or closed options requested.
4. Email addresses (and other personal data) should not be passed on without the consent of the owner.

Implementation issues

1. It is acknowledged that, hitherto, practice has not been so structured – so there may be instances where a closed option is requested, but the email address has already been made visible to the group.
2. I am transitioning from iMail and iCal to Outlook. Whilst the bcc facility is available for emails in iMail, I have not found any way to hide meeting invitees in iCal invites. The Outlook option covers both requirements.
3. I will use the starting assumption, based on these constraints, that everyone's current status is **open**.