The United Reformed Church

Ministries
The United Reformed Church
86 Tavistock Place, London WC1H 9RT

URC Confidentiality Policy

Papers H1 Assembly Executive 2021 and updated H4 General Assembly 2022

1. Introduction

1.1 The United Reformed Church affirms that the church should be a place of trust and safety for everyone, whether they are church members or not.

1.2 The United Reformed Church keeps and uses personal data for the purpose of general church administration e.g. pastoral care and oversight including calls and visits, ministry to children and young people, preparation of rotas, maintaining financial records, safeguarding vulnerable groups, training and to contact people to communicate church news, events and activities. This data may be held by the United Reformed Church at local church, Synod and General Assembly levels. It can be held in paper filing systems and in computer databases. Data is kept by the United Reformed Church under the Data Privacy Notice and disclosed to other church leaders, administrators, Synod Officers and pastoral visitors as necessary to facilitate the administration and ministry of the church activities whether at local church, Synod or General Assembly.

1.3 This policy asks everyone to be aware of the information they hold about other people and explains the expectations of the denomination in relation to confidentiality. The policy provides guidance notes to those who will be receiving, handling and storing personal, criminal convictions data and "special category" (formerly termed "sensitive") data.

1.4 It is important to read this policy alongside the Data Privacy Notice which specifies how your data is used and can be found at https://urc.org.uk/images/EL_Privacy_notice.pdf

2. The purpose of the policy

2.1 The purpose of this policy is to set out clearly the procedures and principles to be used by anyone who exercises a role within, or on behalf of, the United Reformed Church when dealing with confidential and personal information whether in the context of local church, Synod or Assembly and whether the person concerned is a volunteer, paid member of staff or an Office Holder, voluntary or paid (hereafter known as worker).

2.2 This policy explains the expectations of those who exercise a role within, or on behalf of, the United Reformed Church in how to treat confidential information. It is unavoidable that those who exercise such roles shall receive and handle personal and private information about others. The United Reformed Church aims to ensure this information is well-protected.

2.3 This policy gives clarity about when personal information is required and to ensure that

- information is relevant to the purpose and not excessive;
- information is accurate;
- personal data collected for one purpose should not be used for another purpose;
- confidential and/or personal information is kept securely; and
- individuals will have access to their own personal data held either in paper form or electronically.

3. Legislative Framework

The United Reformed Church will monitor this policy to ensure it meets statutory and legal requirements including Data Protection Act 2018, Children's Act 1989, Rehabilitation of Offenders Act 1974, Prevention of Terrorism Act 2000, and Social Security Administration (Fraud) Act 1997 and subsequent legislation that affects confidentiality.

4. Exceptions

To establish a relationship of trust within a pastoral relationship and within the wider church community, it is important that the things people share are treated in confidence. There are three exceptions to this:

- If someone specifically gives the worker permission to pass on something they have said (e.g. they give permission for a situation they are facing to be mentioned in the intercessions at church).
- If a person discloses information that leads a worker to think that the person or another person is at risk.
- If a person indicates that they have been involved in or are likely to become involved in the commission of a criminal offence.

4.1 For the avoidance of doubt in the second and third cases information should be passed on to the Church Safeguarding Coordinator, Synod Safeguarding Officer, or agency immediately.

a) where the Church has a statutory duty to disclose information, (e.g. if there is a safeguarding concern);
b) in exceptional circumstances where there is evidence or reasonable cause to believe that an individual is suffering, or is at risk of suffering, neglect or physical, mental or

other disability, age, illness, or other situation are permanently, or for the time being, unable to take care of themselves, or to protect themselves against significant harm, abuse or exploitation." (GP5 5.1 p29 onwards); Care Act 2014;

c) to prevent significant harm to a child or harm to an adult;
d) where seeking consent would prejudice the provision of the protection, the prevention, detection or prosecution of a crime;
e) where seeking consent could delay the enquiry process into allegations of significant and harm;
f) where an accused minister in the United Reformed Church's Disciplinary process for Ministers of Word and Sacraments and Church Related Community Workers discloses information that is pertinent to the case against them to their pastoral support which is both a safeguarding concern or may be an admission of misconduct or gross misconduct.

4.2 Wherever possible the person disclosing information should be supported in sharing that information himself or herself. If that is not likely, they should be encouraged to give permission for the information to be passed on. The worker may only disclose the information to the appropriate third party without permission where the two options mentioned are not possible. A child would not necessarily be expected to disclose information themselves, but they should be carefully consulted. Guidance on the Safeguarding of Young People and adults at risk can be found on the URC website and in Good Practice 5 - page 73ff.

4.3 Where there is an indication by an individual, that things verbally mentioned ought to be kept confidential, the expectation is that this is understood and adhered to (subject to the circumstances outlined above).

5. Responsibilities

5.1 Church House

Church House staff, Office Holders and volunteers will operate this policy in line with the Data Privacy Notices of their departments.

5.2 Synods

Synod staff, Office Holders and volunteers will operate this policy in line with the Data Privacy Notices of their Synods.

5.3 Elders and Church Meetings

Elders, church members and volunteers will operate this policy in line with the Data Privacy Notices of their church.

- The limits of confidentiality within any Elders or church meetings needs to be identified and not kept by implicit assumption but by an explicit and agreed policy. All meetings will remain in good order, where there is an application of the data protection principles. In particular, knowing that information should only be shared where permission is provided by the owner, or it is in the public domain and the person involved knows the context in which their information will be passed on.
- Where there are group discussions about an individual's status, participants of the said groups must be reminded of the confidential nature of their business.
- Elders should have their own email accounts, rather than sharing with a partner. Shared email accounts constitute a breach of confidentiality, and data protection laws.

5.4 Committees

All Committee members (local churches, Synods or General Assembly) of the United Reformed Church, are required to sign the Data Privacy Committee form, both when joining and leaving the committee. These forms should be in the possession of the secretary of the committee.

5.5 Prayer Support

In the instances of vocalised prayers during a church service, prayers written in books, hung on prayer trees, and passed on to prayer chain networks, several things must be taken into consideration, to ensure compliance of data protection law. Below is an outline of what local churches should consider, when offering prayer support to the congregation.

5.5.1 Where a member might reasonably expect and welcome prayers from the local church, it is not necessary to obtain their consent for processing prayer requests on their behalf. The local church must be able to justify processing a member's health data (i.e., having a legitimate reason where health information is shared during prayers). Prior to disclosing information about a parishioner's health, consideration must be given to the sensitivity of the information and the impact on the member and their family, if that information was publicised (for example, information about a terminal illness – it would be expected that expressed consent is sought).

5.5.2 Where there isn't a legitimate reason/interest for processing a member's health data, it may be advisable to either:

- pray for the member by mentioning their name only, and nothing else (on the basis they might reasonably expect and welcome prayers).
- pray about the illness, without making mention of the member (i.e., anonymisation); or

- try to obtain expressed consent from the member, as health information is sensitive personal data. Where the member is unable to give expressed consent, consent can be sought from family members, as they will be able to decide on behalf of the member.

5.5.3 When processing member's personal information, please consider the following, in accordance with the UK GDPR.

- Data minimisation – what is the minimum information needed for a person and their health condition to pray for them?
- Data security – how much personal information is provided verbally, printed, or disclosed in various networks?
- An individual's right of objection – how does an individual get themselves removed from the prayer list/tree and what would that entail?

5.5.4 When a Minister, a Locally Recognised Worship Leader or an Assembly Accredited Lay Preacher invites topics for intercessory prayers, it's vitally important that individuals understand nothing can be shared about an individual, without their expressed consent. However, information that is already in the public domain about someone being prayed for, can be shared with others, because it is accessible to all. Information publicly known cannot be given personal data protection rights, under data protection laws.

5.6 Writing References

The information below relates to providing a *professional* reference.

Information given in a reference is usually based on the suitability of an individual for a specific role, as described in a job description and/or person specification. It should be an accurate assessment, to the best of knowledge and understanding, as to whether the candidate has the qualifications, skills and aptitudes to do the job as described.

As a referee you owe the subject of the reference a duty to take reasonable care to ensure the information it contains is true, accurate and fair and does not give a misleading impression. Any opinions should be supported with facts.

It is advisable to avoid referring to any matter relating to any of the protected characteristics mentioned in the Equalities Act 2010. (for example: the primary reason for not disclosing information about health record is to avoid any potential claim for discrimination on grounds of disability).

Under the current data protection legislation, individuals are not entitled to access a confidential employment reference written about them. To refuse disclosure, the reference should clearly state that it is confidential, intended for the attention of the recipient only and that the author does not give permission for it to be disclosed to the subject. With the foregoing statement the reference would not be accessible to the candidate. That said, any reference being freely given on request, should not contain within it any information that you, as the referee, would not stand by.

6. Breaches of confidentiality

Any breach of confidentiality will be dealt with, in accordance with the disciplinary policy put in place, in the various categories of workers (i.e., employees, officer holders, Ministers of Word and Sacraments and Church Related Community Workers) in the URC.

7. Support for those working in pastoral care

Support should be provided to individuals in a recognised pastoral relationship. Churches and/or Synods should have an effective system in place, that provides support for individuals engaging in pastoral work. It would be ideal if they were given an opportunity to converse with a professional such as a Synod Safeguarding officer or other individuals, such as an experienced pastoral visitor, a pastoral secretary, a lay pastoral worker, a minister, or church related community worker.

Appendix 1
Guidelines for Good practice in Confidentiality and Pastoral Care

1. There are three simple headings which can help individuals in pastoral relationships to develop their self-awareness in relation to confidentiality.

i) When to tell

- When permission has been given by the 'owner of the story'.
- When an individual/individuals will be at risk of harm if the information is not passed on.
- When information has been disclosed about a criminal offence that has taken place or is planned.
- In the context of an Elders meeting when sharing pastoral news, with an awareness of the individual's prior knowledge that this may take place.
- Safeguarding concerns should always be shared in line with their church's policy, usually with the pastoral worker's line manager or church safeguarding coordinator

in the first instance, or the Synod Safeguarding Officer, except in emergency situations. It is the responsibility to share a concern with an at-risk individual, as long as the individual or other person is not put at an increased amount of risk by this action.

ii) What to tell

- What are the facts of the story? These need to be told without gloss or 'spin'. Be careful to use words that were used and do not place your own interpretation on what was said.
- Personal information such as an individual's name or mentions of their personal matters should only ever be mentioned during public worship and in the context of open prayers, where expressed consent or permission was given by the said individual. This applies to prayers written in books, hung on prayer trees and passed on to prayer chains and networks.
- Care should be taken when a worship leader or preacher invites topics for intercessory prayer. Everyone must be aware that they should only share information about other individuals, where permission (by those individuals) has been given.
- Avoid sharing more than is necessary. Ensure that disclosure of information is proportionate to the aim of sharing (Human Rights Act, proportionate and necessary).

iii) Who to tell

- Identify the most appropriate person (if any) to pass on the information to. The following questions should be considered: Who can help or has the resources or access to support for the person concerned? Who will most appropriately support the pastoral worker in reflecting on what they have heard?
- Ministers, Church Safeguarding Coordinators, Elders, Synod Safeguarding Officers or other local church leaders will need to make decisions about sharing information with external agencies, including the Police and Local Authority. Individuals may not give their consent to the sharing of safeguarding information for several reasons. For example, they may be frightened of reprisals, they may fear losing control, they may not trust social services, or other partners, or they may fear that their relationship with the abuser will be damaged. Reassurance, appropriate support and advice from a safeguarding professional may provide guidance to the individual in these circumstances, in order for them to make an informed decision about the sharing of information. Advice can be sought from Synod Safeguarding Officers or Designated Safeguarding Lead.

- Identify any persons or groups who should not be told. It should not be assumed that the person concerned has told their family or friends. Potential harm could be done if someone was to contact the individual's family.
- It is not good practice for pastoral workers to share pastoral information about third parties with members of their family. People would not expect a GP to pass on to their partner confidential medical information, yet often assumptions are made that to tell a pastoral worker information will lead automatically to their partner knowing. Boundaries of confidentiality need to be made clear to all concerned, and the family members of the person offering care should not be expected to carry the responsibility of holding such information.

Appendix 2
Guidelines for the use of Technology

1. Technology

1.1 Data storage

When a computer is passed on, sensitive and confidential data from the hard drive should be permanently deleted. Security software can be purchased to do this. Alternatively, hard drives should be removed from equipment being disposed of.

Where data is stored in such a way that there is shared access, proper use of passwords should be made to limit access to appropriate persons. This is true of those whose computers are based at home and used by family members, as well .as those who work in an office.

When data is stored on portable media, including: CD and DVD ROMs, Cloud drives, USB drives, mobile phones and laptops, care needs to be taken to password protect files and machines. Passwords should be stored securely and form part of the Business Continuity Plan.

If using a Wireless Local Area Network (WLAN) to store, send or receive confidential information, it is important to ensure that a high level of security encryption is enabled.

1.2 Social Media Networks and Websites

Sites such as Facebook and Instagram and popular others are increasingly popular and are used by many people as a source of support and friendship. People are often quite relaxed about the amount of information they disclose about themselves and possibly about

others. It is important to apply the principle of 'who owns the story' in what is shared about others online, remembering not to share if it is not about yourself.

1.3 **Photocopiers**

Be mindful of leaving sensitive material on the photocopier, especially original documents. Others using the photocopier after you, may not understand the importance of the document and/or the severity of the confidential nature of what has been left for all to see. Be aware thar some photocopiers retain a scan of a document until the next document has been copied in its memory. If a print run is interrupted (due to lack of ink or paper), be sure to restock whatever is required. Leaving the restocking task to someone else, could result in confidential information falling into the wrong hands. Restricted access must be placed on sensitive information.

1.4 Email

Individuals should have their own email addresses otherwise confidentiality is immediately breached as both parties (if there is a marriage or partner relationship) have access to the information sent, for one person's viewing only.

Any email that contains personal data about a third party should only be sent with their permission and should be treated with the same care and attention as any other written information being passed on.

It is important to take care not to accidentally 'reply to all', if the contents of your reply to an email should not appropriately be seen by the wider group. When emailing a group, if the members have not given permission for their details to be circulated within the group, they should be mailed using the 'blind carbon copy' (i.e. bcc) facility.

1.5 **Protecting contents**

When sending documents, secure the contents against accidental or deliberate alteration by converting documents into a more secure format such as a PDF. Ideally you should encrypt emails sent. Containing documents attached. The password should be sent in a separate email.

1.6 Mobile Technology

The same care should be taken in passing on texts as when using any other method of passing on information. It is important not to discuss personal details of individuals whilst using a mobile phone in a public place.

Documents, images, sound recordings and videos can easily be made and passed on using various kinds of mobile technology. If sending data by Bluetooth it is important to remember that unintended people may have their Bluetooth connectivity set to 'on' and be able to receive information. When sending confidential or potentially sensitive data it is important to target a particular device (phone or laptop), rather than use a general broadcast, which may be picked up by other devices within range.

1.7 Shredding

The increase in cases of identity theft has brought to light the need for careful disposal of sensitive or personal information in accordance with the relevant retention schedule.

Documents containing personal details or confidential information should be shredded before binning or recycling.

1.8 Virtual Conferencing Platforms

Virtual Conferencing Platforms (such as Zoom, Lifesize and Teams) are approved software tools for conducting remote/virtual meetings. This document provides basic guidance on how to protect your privacy and the privacy of others when using Zoom:

1.8.1 Visibility of Remote Work Locations: Participants should use the platform's virtual background feature, when available, if they do not want to have their surroundings visible.

1.8.2 Screen Sharing Privacy

- **Protecting Confidential Data on Your Device from Being Viewed**: Avoid sharing confidential information visible on your other screens. Before screen sharing, close all applications, emails and documents that you will not use in that session.

- **Managing whose screen is visible**: Default settings should be set to limit screen sharing to the host. The host can also allow screen sharing by participants. The host can select the "host only" setting to prevent others from sharing their screens. If the host determines that screen sharing by participants is needed, sharing by "one participant at a time" should be selected. The host should remind participants not to share other sensitive information during the meeting inadvertently.

1.8.3 Managing Participants Some basic tips for limited preventing unwanted attendees or 'Bombing' are listed below:

- Don't post meeting IDs in public forums.
- Don't reuse meeting access codes. You can generate a new access code for each meeting.
- Set a password for the meeting

- Monitor participant list for unwanted attendees
- Set up a waiting room function

1.8.4 Zoom recordings. When you record a meeting and choose Record to the Cloud, the video, audio, and chat text are recorded in the Zoom cloud. Prior to you recording a meeting, you must obtain consent from all meeting attendees. The recording files can be downloaded to a computer or streamed from a browser. Recordings can also be password protected, restricting their visibility to selective people. Cloud recordings allow you to record the meeting in multiple different recording layouts including active speaker, gallery view, and shared screen, and can be configured with a variety of cloud recording storage options. If a meeting host enables cloud recording and audio transcripts, both will be stored encrypted.

1.8.5 Retention period: Zoom cloud recordings are retained for 180 days. Any recordings older than 180 days (from the recording date), will be deleted from Zoom's cloud storage service. It is advisable that meetings are downloaded and stored on your servers, in a secure folder, if you wish to retain them longer than 180 days. The onus will then be on you, to ensure you only keep recordings in accordance with your local retention schedule period.