Paper H1

URC Confidentiality Policy

Ministries Committee

Basic information

Contact name and email address	The Revd Paul Whittle moderator@urcscotland.org.uk
Action required	Decision.
Draft resolution(s)	**Assembly Executive adopts the URC Confidentiality Policy.**

Summary of content

Subject and aim(s)	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.
Main points	This policy gives clarity about when personal information is required and ensures that those who handle information on behalf of the URC make sure 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. The policy sets out guidance on how this can be achieved.
Previous relevant documents	Good Practice 5.
Consultation has taken place with...	HR, URC Compliance Officer, URC Legal Adviser, Synod Safeguarding Officers.

Summary of impact

Financial	None.
External (e.g. ecumenical)	

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 eg 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 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 relevant Data Privacy Notices which specifies how your data is used. These can be found in your local congregation; for synods, on synod websites, and for the General Assembly at: **https://urc.org.uk/privacy-notices**

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.

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
- 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, (i.e. 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 p15); 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

- 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. A 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

Personal information such as an individual's name and other personal identifiers should not be mentioned in public worship and in the context of open prayers if express consent and permission is not provided by the individual. This is applicable in the instances of prayers written in books, prayers hung on prayer trees and prayers passed on to prayer chain groups and networks. Personal data is fragile and so care must be taken to only share, where permission has been given by the person who the data belongs to.

When a Minister, a Locally Recognised Worship Leader or an Assembly Accredited Lay Preacher invites topics for intercessory prayers, it's vitally important that people understand nothing can be shared about an individual, without their consent. They could, however, share information that is already in the public domain, about the individual, that is available for all to see. Information publicly known cannot be given personal data protection rights, under data protection laws.

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' (ie 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.