



Data & Communications Policy

Policies/Notices to include:

Privacy Notice, Processing Document, Data Breach Management Document, Conflict of Interest Policy

Policy Owner: Business Group

Version	
November 2023	Implemented
August 2025	Changes to Clerk

Privacy Notice

Privacy Notice
The Presbytery of Cleir Eilean I: Highlands and Hebrides Scottish Charity Number
SC001424

The Presbytery of Cleir Eilean I: Highlands and Hebrides Scottish Charity Number SC001424 (the 'Presbytery') is providing you with this Privacy Notice in order to comply with data protection law and to ensure transparency in the collection and use of your personal data.

Who is collecting the information

The Presbytery is the Data Controller. The main contact for queries in relation to this processing is Presbytery Clerk or the Presbytery Support Officer, you can contact them by email at CleirEileanI@churchofscotland.org.uk

Why is this personal data collected and for what reason (Purpose)

This information is used to:

- administer membership records
- enable pastoral care
- for the general oversight of Church of Scotland congregations within the Presbytery
- enable participation in Presbytery activities including the training and supervision of ministers, candidates for the ministry and probationers
- provide you with information about news, events, and activities within the Presbytery or the wider Church of Scotland
- fulfill legal obligations
- further charitable aims, for example through fundraising activities
- maintain accounts and records (including the processing of Gift Aid applications)
- comply with safeguarding obligations including, the protection of vulnerable groups scheme
- maintain a directory of contact details

What personal data is collected

Personal data will include only what is necessary to fulfill the purposes listed. For most members it will only include name, address and contact details supplied.

- Name
- Address
- Telephone number
- Mobile number
- Date of Birth
- Email address
- Bank details (for Gift Aid and fundraising purposes)
- Children's data (for example, but not limited to, if required for instance for Junior Church, holiday clubs or baptism)
- Role in Church (e.g. office-bearer information)
- Health-related information
- Photographs and videos (where applicable)
- Safeguarding information, including Covenant of Responsibilities
- Religious beliefs are collected by implication by being a church member

The information source

The information is collected directly from you. Some data is collected via your congregation or the National Offices.

The lawful basis for the processing

The Presbytery processes special category (sensitive) information under UK GDPR Article 9(2)(d) *“processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects”*.

For the other processing activities, the lawful basis are:

- UK GDPR Article 6(1)(c) *“processing is necessary for compliance with a legal obligation to which the controller is subject”*;
- UK GDPR Article 6(1)(f) *“processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child”*.
- UK GDPR Article 6(1)(a) *“the data subject has given consent to the processing of his or her personal data for one or more specific purposes.”* This is specific to safeguarding purposes.

Who personal data is shared with

Your personal information will only be shared where this is necessary for the purposes set out above. Information will not be shared with any third party out with the Church of Scotland without your consent unless the Presbytery is obliged or permitted to do so by law.

The Presbytery uses the following third party suppliers (processors) Microsoft, Sanctus Media, Zoom and Adobe Acrobat to process your personal data. There is appropriate contracts in place and data will only be processed in accordance with the instructions of the Presbytery.

How long the personal data is held for

The Presbytery will keep your personal information for as long as you are a member or adherent, or have regular contact with the Presbytery, or for as long as the Presbytery is obliged to keep it by law or may need to do so in order to respond to any questions or complaints or to show that the Presbytery treated you fairly. When the information is no longer needed it will be securely destroyed following church procedure. Further information about our retention and disposal schedule is available on our website.

Individuals’ rights in relation to this processing

Under data protection laws, individuals have a number of rights in relation to the processing of their personal data. These rights are as follows:

- The right to be informed – this privacy notice meets that right.
- The right of access – this means you have the right to have access or receives copies of personal data held by the organisation
- The right to rectification – this means you have the right to correct incomplete or inaccurate data held about you
- The right to erasure – this means you have the right to have your data deleted from an organisation’s records.
- The right to restrict processing – this means you have the right to restrict processing. This right is normally used with other rights, e.g. rectification
- The right to data portability – this means you have the right to request your data in a machine-readable format (e.g. a .csv file) and transfer this to another organisation

- The right to object – this means you have the right to object to how your data is processed
- Rights in relation to automated individual decision making, including profiling – the Church does not carry out this type of processing.

Not all rights apply and it depends on the lawful basis as to what rights do apply.

For the processing purposes of this privacy notice, when the lawful basis is legal obligation the right of erasure, right to data portability and the right to object do not apply. All other rights do apply. For the processing purposes of this privacy notice when the lawful basis is legitimate interests, all rights apply except for data portability. If you wish to exercise any of your rights the main contact for queries in relation to this processing is Presbytery Clerk or Presbytery Support Officer via email at CleirEileanI@churchofscotland.org.uk, they will process your request accordingly.

If any processing is carried out on the basis of consent, it is important to note that you can **withdraw your consent** at any time. To do this please contact Presbytery Clerk or Presbytery Support Officer via email at CleirEileanI@churchofscotland.org.uk

Complaints to the Church of Scotland

If you are concerned about how your personal data is being used by the Church of Scotland, please contact - in the first instance - the main contact for queries in relation to this processing, Presbytery Clerk or Presbytery Support Officer via email at CleirEileanI@churchofscotland.org.uk. You can also contact the Church of Scotland Data Protection Officer (DPO) at Privacy@churchofscotland.org.uk if required.

Complaints to the Information Commissioner's Office (ICO)

If you are not satisfied with the outcome of your complaint to the Church of Scotland, a referral can be made to the UK regulator of data protection, the Information Commissioner's Office (ICO). The website details how to contact them and your rights: <https://ico.org.uk/for-the-public/>

Further information

If you would like further information in relation to this Privacy Notice please contact the Church of Scotland Data Protection Officer (DPO) at Privacy@churchofscotland.org.uk

This Privacy Notice may be updated from time to time to reflect changes in legal requirements or other operational reasons. The latest version will always be available from the Presbytery of Cleir Eilean I: Highlands and Hebrides, Scottish Charity Number SC001424.

The Presbytery of Cleir Eilean I: Highlands and Hebrides Scottish Charity Number SC001424

The Presbytery of Cleir Eilean I: Highlands and Hebrides Scottish Charity Number SC001424 (the 'Presbytery') is providing you with this Privacy Notice in order to comply with data protection law and to ensure transparency in the collection and use of your personal data.

Who is collecting the information

The Presbytery is the Data Controller. The main contact for queries in relation to this processing is Presbytery Clerk or the Presbytery Support Officer, you can contact them by email at CleirEileanI@churchofscotland.org.uk

Why this personal data is collected and for what reason (Purpose)

The Presbytery collects and processes your personal data for employment purposes. Processing employee data allows the Presbytery to:

- run recruitment processes, including promotion processes
- maintain accurate and up-to-date employment records and contact details (including details of who to contact in the event of an emergency) and records of employee contractual and statutory rights
- operate and keep a record of disciplinary and grievance processes in order to ensure acceptable conduct within the workplace
- operate and keep a record of employee performance and related processes in order to plan for career development, succession planning and workforce management
- operate and keep a record of absence and absence management procedures in order to allow effective workforce management and ensure that employees are receiving the pay or other benefits to which they are entitled
- obtain occupational health advice in order to ensure compliance with duties in relation to individuals with disabilities, comply with health and safety law and ensure that employees are receiving pay or other benefits to which they are entitled
- operate and keep a record of other types of leave (including maternity, paternity, adoption, parental and shared parental leave) in order to allow effective workforce management, ensure compliance with duties in relation to leave entitlement, and to ensure that employees are receiving the pay or other benefits to which they are entitled
- ensure effective business administration;
- provide references on request for current or former employees
- respond to and defend against legal claims and
- maintain and promote equality in the workplace.

What personal data is collected

The Presbytery collects and process a range of information about you. This includes:

- name, address, date of birth, gender and contact details (including email address and telephone number);
- the terms and conditions of your employment;
- your qualifications, skills, experience and employment history, including start and end dates of previous employment and employment within the organisation;
- information about remuneration, including entitlement to benefits such as pensions, childcare vouchers or insurance cover;
- your bank account and national insurance number;
- information about your marital status, next of kin, dependants and emergency contacts;
- information about your nationality and entitlement to work in the UK;
- information about any criminal record you may have;

- details of your schedule (days of work and working hours) and attendance at work;
- details of periods of leave taken by you including holiday, sickness absence, family leave and sabbaticals and the reasons for the leave;
- details of any disciplinary or grievance procedures in which you have been involved including any warnings issued to you and related correspondence;
- assessments of your performance including appraisals, performance reviews/ratings, training you have participated in, performance improvement plans and related correspondence;
- information about medical or health conditions including whether or not you have a disability for which the organisation needs to make reasonable adjustments;
- details of trade union membership; and
- equal opportunities monitoring information, including information about your ethnic origin, sexual orientation, health and religion or belief.

Some of this data is special category (sensitive) personal data and therefore additional safeguards are put in place to protect this data further. Special category data is defined as racial/ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health data, genetic data, biometric data, sex life, sexual orientation.

The information source

The information is collected in a variety of ways. Some information is collected directly from you. Other sources can include: third parties for references, PVG checks with Disclosure Scotland, application forms, CVs or resumes, passport or other identity documents such as driving licence, forms completed by you at the start of or during employment, from correspondence with you or through interviews, meetings or other assessments.

The Presbytery may also collect personal data about you from third parties, such as references supplied by former employers and, where applicable, information from criminal records checks permitted by law.

The lawful basis for processing

The lawful basis for processing for employment purposes is UK GDPR Article 6(1)(b) *“processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract”*.

There are some aspects of processing where the lawful basis is UK GDPR Article 6(1)(c) *“processing is necessary for compliance with a legal obligation to which the controller is subject”*. This is in relation to checking employee’s right to work in the UK, tax deduction, health and safety and criminal records check/PVG to ensure that individuals are permitted to undertake the role in question.

Where special category (sensitive) personal data is involved, the lawful basis for processing is UK GDPR Article 9(2)(b) *“processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by domestic law or a collective agreement pursuant to domestic law providing for appropriate safeguards for the fundamental rights and the interests of the data subject”*

Who the information is shared with:

Your information will be shared internally, including with members of the Presbytery, your line manager and the National Office.

The Presbytery may share your data with third parties in order to obtain pre-employment references from other employers and obtain necessary criminal records checks from Disclosure Scotland.

The Presbytery uses the following third-party suppliers (processors) Microsoft, Sanctus Media, Zoom and Adobe Acrobat to process your personal data. There is appropriate contracts in place and data will only be processed in accordance with the instructions of the Presbytery.

How long the personal data is held for

The Presbytery will hold your personal data for the duration of your employment. The periods for which your data is held after the end of employment are set out in the Retention and Disposal Schedule available on our website.

Individuals' rights in relation to this processing

Under data protection laws, individuals have a number of rights in relation to the processing of their personal data. These rights are as follows:

- The right to be informed – this privacy notice meets that right.
- The right of access – this means you have the right to have access or receives copies of personal data held by the organisation
- The right to rectification – this means you have the right to correct incomplete or inaccurate data held about you
- The right to erasure – this means you have the right to have your data deleted from an organisation's records.
- The right to restrict processing – this means you have the right to restrict processing. This right is normally used with other rights, e.g. rectification
- The right to data portability – this means you have the right to request your data in a machine-readable format (e.g. a .csv file) and transfer this to another organisation
- The right to object – this means you have the right to object to how your data is processed
- Rights in relation to automated individual decision making, including profiling – the Church does not carry out this type of processing.

Not all rights apply and it depends on the lawful basis as to what rights do apply. For the processing purposes of this privacy notice the right to object does not apply. All other rights do apply. If you wish to exercise any of your rights the main contact for queries in relation to this processing is Presbytery Clerk or Presbytery Support Officer via email at CleirEileanI@churchofscotland.org.uk, they will process your request accordingly.

If you are concerned about how your personal data is being used by the Church of Scotland, please contact - in the first instance - the main contact for queries in relation to this processing, Presbytery Clerk or Presbytery Support Officer via email at CleirEileanI@churchofscotland.org.uk. You can also contact the Church of Scotland Data Protection Officer (DPO) at Privacy@churchofscotland.org.uk if required.

Complaints to the Information Commissioner's Office (ICO)

If you are not satisfied with the outcome of your complaint to the Church of Scotland, a referral can be made to the UK regulator of data protection, the Information Commissioner's Office (ICO). The website details how to contact them and your rights: <https://ico.org.uk/for-the-public/>

Further information

If you would like further information in relation to this Privacy Notice please contact the Church of Scotland Data Protection Officer (DPO) at Privacy@churchofscotland.org.uk

This Privacy Notice may be updated from time to time to reflect changes in legal requirements or other operational reasons. The latest version will always be available from the Presbytery of Cleir Eilean I: Highlands and Hebrides, Scottish Charity Number SC001424.

The Church of Scotland Presbytery of Cleir Eilean I (“the Presbytery”)
Data Protection Breach Incident Management Policy

This policy covers all congregations within the Presbytery.

Data protection laws include a data breach reporting requirement to the regulator, the UK Information Commissioner’s Office (ICO) and, potentially, informing affected individuals if there is a risk to their rights and freedoms. There are different types of breaches and this policy will provide further guidance and detail the process for reporting a breach and the action that must be taken as quickly as possible. If a breach is reportable, we only have 72 hours from breach discovery to report it to the ICO and (potentially) to the affected individuals.

Under data protection laws a data breach is defined as *“a breach of security leading to the unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.”* Breaches can be classified under three categories:

- Confidentiality breach – this is an unauthorised or accidental disclosure of or access to personal data. This is the most common type of breach.
- Integrity breach – this is an unauthorised or accidental alteration of personal data
- Availability breach – this is an accidental or unauthorised loss of access to, or destruction of personal data.

If it appears that a data breach has occurred, the breach notification form must immediately be completed and sent both to the Presbytery Clerk and to the Data Protection Officer (DPO) at the National Office. The following breach management plan will then be implemented.

1. Containment and recovery

1.1 The Presbytery Clerk as Data Protection Compliance Officer will take the lead in responding to the breach, including liaising with the DPO and the individuals who have reported the incident. It will be necessary to investigate the nature and cause of the breach and the extent of the harm that could result. The Presbytery Clerk may elect to carry out all necessary investigation him or herself or alternatively may appoint someone else to do so. As a first step, the Clerk will establish who needs to be made aware of the breach and will inform them of what they are expected to do to assist in the containment exercise. This could be, for example, finding a lost document or piece of equipment.

1.2 Steps must be taken to establish whether there is anything which can be done to recover any losses and limit the potential damage arising from the breach. As well as the physical recovery of equipment, this could involve the use of back up tapes to restore lost or damaged data or ensuring that people recognise when someone tries to use stolen data to access accounts.

1.3 The Clerk will determine the identity of the controller for the purposes of the breach, bearing in mind that there may be more than one controller where shared services are involved. If it appears that the breach has been caused by another controller, or by the processor, the terms of the contract with that third party will be checked with a view to determining whether a claim may lie for breach of a specific obligation, breach of confidence or a failure to take reasonable skill and care; and whether the breach gives rise to a right to terminate the contract.

- 1.4 An immediate report of the breach must be made by the Clerk to the Data Protection Officer (DPO) of the Church.
- 1.5 Consideration should be given to whether or not it is appropriate to inform the police.

2. Assessing the risks

2.1 Some data security breaches will not lead to risks beyond possible inconvenience to those who need the data to do their job. Before deciding on what steps are necessary beyond immediate containment, the Clerk will assess the risks which may be associated with the breach. Perhaps most important is an assessment of potential adverse consequences for individuals; how serious or substantial these are; and how likely they are to happen.

2.2 The following points will be borne in mind when making this assessment:

- What type of data is involved? For example, contact details, congregation or Presbytery data.
- Some data is sensitive (and classed as special category¹ under data protection law) because of its very personal nature (e.g. information about health, or religious beliefs) while other data is considered sensitive because of what might happen if it is misused (financial details could lead to fraud)
- If data has been lost or stolen, are there any protections in place such as encryption?
- What has happened to the data? If data has been stolen, it could be used for purposes which are harmful to the individuals to whom the data relates; if it has been damaged, this poses a different type and level of risk
- Regardless of what has happened to the data, what could the data tell a third party about the individual? Sensitive data could mean very little to an opportunistic laptop thief while the loss of apparently trivial snippets of information could help a determined fraudster build up a detailed picture of other people and enable identity theft to occur
- How many individuals' personal data are affected by the breach? It is not necessarily the case that the biggest risks will accrue from the loss of large amounts of data but this is an important determining factor in the overall risk assessment
- Who are the individuals whose data has been breached? Whether they are staff, volunteers or suppliers, for example, will to some extent determine the level of risk posed by the breach and, therefore, the appropriate actions in attempting to mitigate those risks
- What harm can come to those individuals? Are there risks to physical safety or reputation, of financial loss or a combination of these and other aspects of their life?
- Are there wider consequences to consider such as a loss of public confidence or reputation?
- If individuals' bank details have been lost, the banks themselves could be contacted for advice on anything they can do to help prevent fraudulent use.

3. Notification of breaches

3.1 Informing people and organisations of the data breach can be an important element in a breach incident management policy, but this is not an end in itself. Notification should have a clear purpose, whether this is to enable individuals who may have been affected to take steps to protect themselves or to allow the appropriate regulatory bodies to perform their functions, provide advice and deal with complaints.

3.2 All decisions on notification will be taken by the Data Protection Officer (DPO), in discussion with the Clerk. The DPO will be responsible for notifying the Information Commissioner's Office ("ICO") where this is appropriate. The Clerk will be responsible for notifying affected individuals, where appropriate.

3.2 If it is likely that there will be a risk to people's rights and freedoms, the breach must be reported to the ICO. If such a risk is unlikely then it does not have to be reported. If a decision is taken not to report the breach, this decision and the reasons for it must be documented. Notifiable breaches must be reported to the ICO without undue delay, but **not later than 72 hours** after discovery of the incident. If we take longer than this, we must give reasons for the delay.

3.3 If a breach is likely to result in a high risk to the rights and freedoms of individuals, those concerned must be informed without undue delay. In other words, this should take place as soon as possible.

A 'high risk' means that the threshold for informing individuals is higher than for notifying the ICO. It will be necessary to assess both the severity of the potential or actual impact on individuals as a result of a breach and the likelihood of this occurring. If the impact of the breach is more severe, the risk is higher; if the likelihood of the consequences is greater, the risk is higher. In such cases, we must promptly inform those affected, particularly if there is a need to mitigate an immediate risk of damage to them.

3.4 The following considerations will be taken into account in assessing the likelihood and severity of the risks and deciding whether to notify:

- The type of breach
- The nature, sensitivity and volume of the data involved
- Ease of identification of individuals
- Severity of consequences
- The number of affected individuals
- Are there any legal or contractual requirements to do so, for example if a regulatory body is involved (is a report of a serious incident to OSCR required?)
- Can notification help the individual? Bearing in mind the potential effects of the breach, could individuals act so as to mitigate risks, for example by cancelling a credit card or changing a password?
- Special characteristics of the individual
- How notification can be made appropriate for particular groups of individuals, for example vulnerable adults
- Is there a danger of 'over notifying'? Not every incident will warrant notification and notifying a large number of people about an issue affecting only a small number may well cause disproportionate enquiries and work

3.5 Bear in mind that it may also be appropriate to notify insurers of potential claims.

3.6 Consideration will also be given to what should be said to any person or body to whom notification is made, and how that message is to be communicated. This will depend to a large extent on the nature of the breach but the following points will be taken into account:

- There are a number of different ways to notify those affected. The most appropriate one will be used, bearing in mind the security of the medium as well as the urgency of the situation
- Notification will include a description of how and when the breach occurred; what data was involved; and what has already been done to respond to the risks posed by the breach
- When notifying individuals specific and clear advice will be given on the steps they can take to protect themselves and also what the Church is willing to do to help them
- Information will be provided about how individuals can obtain further information or ask questions about what has occurred

4. Evaluation and response

4.1 It is important not only to investigate the causes of the breach but also to evaluate the effectiveness of the Presbytery's response to it. If it is established that existing procedures could lead to another breach, improvements to those procedures will be identified. Questions to be asked will include:-

- Was the data protection policy, and in particular its security provisions, followed?
- What procedures are in place and can they be improved?
- Does action need to be taken to raise security compliance standards?
- What are the weak points in existing security measures?
- Should disciplinary steps be taken against any staff members?
- Have adequate training and guidance been provided?
- Are adequate contractual safeguards in place?
- Where do the biggest risks lie? Risks will arise when sharing data with or disclosing to others. Are the methods of transmission secure? Is only the minimum amount of data necessary being disclosed or shared?

5. Recording breaches

5.1 All breaches must be recorded, regardless of whether or not they need to be reported to the ICO. All reported breaches to the DPO are recorded, including identifying whether it was reportable to the ICO or individuals. The DPO also records any training needs or lessons learned from the incident. A similar record should be held at Presbytery level.

5.2 The facts relating to the breach, its effects and the remedial action taken must all be recorded. Consideration should be given to whether or not the breach was a result of human error or a systemic issue and how a recurrence might be prevented, whether through better processes, further training or other corrective steps.

November 2023

The Presbytery Of Cleir Eilean I (SC001424) Conflict of Interest Policy

CONTENTS

1. Introduction
2. Scope and Purpose
3. Conflict of interest
 - 3.1 What is a conflict of interest?
 - 3.2 Recognising and disclosing conflicts of interest
4. Procedure
 - 4.2 Register of interests
 - 4.3 Disclosure
 - 4.4 Managing conflicts of interest
 - 4.5 Recording
5. Consequences of breach
6. Review

Appendix 1

Declaration of interest form

1. Introduction

1.1 Conflicts of interest affect all types and size of organisations. In a charity context, a conflict of interest can inhibit free discussion, and can lead to decisions which are not in the best interests of the charity and which are invalid or open to challenge. Conflicts of interest can also be damaging to a charity's reputation and to the public's confidence and trust in charities in general.

1.2 Charity trustees have a primary duty in terms of S.66 of the Charities and Trustee Investment (Scotland) Act 2005 to act in the best interests of the charity at all times.

1.3 Members of the Kirk Session [insert "and members of the Congregational Board/Deacons' Court" if there is one] are the charity trustees of the congregation.

1.4 On occasion, trustees can find themselves in a situation that may give rise to conflicts of interest, whether potential or actual, perceived or alleged. Where trustees can identify a conflict and measures can be put in place to prevent the conflict affecting decision-making then the harmful effects of a conflict of interest can be prevented. The proper handling of conflicts of interest is an essential part of good decision-making by trustees.

1.5 This policy has been developed to provide guidance to all trustees regarding conflicts of interest in order to avoid any actual or potential conflicts of interest, perception of bias or misuse of authority, and to ensure and evidence that all decisions by individual trustees on behalf of the congregation are taken only in the best interests of the congregation at all times.

2. Scope and purpose

2.1 This policy applies to all trustees of the congregation and to all bodies, groups and committees meeting under the auspices of the congregation. All individuals in the congregation who are involved in management of its affairs to a greater or lesser extent but are not members of the Session [or Board/Deacons' Court] can be seen as "shadow trustees" and are subject to the same duties as the trustees. Where the word "trustee" is used in this policy it covers both charity trustees and shadow trustees.

2.2 The congregation is committed to ensuring that all trustees act in its best interests at all times. This policy aims to provide guidance to those involved in management and decisionmaking and seeks to ensure that all trustees are seen to be acting in accordance with well recognised rules of good governance.

2.3 It is inevitable that conflicts of interest will arise. This policy aims to ensure that any conflict is identified and managed appropriately.

2.4 It is the responsibility of each individual to recognise situations in which he or she has a conflict of interest, or might reasonably be seen by others to have a conflict, to disclose that conflict to the appropriate person and to take such further steps as may be appropriate as set out in more detail under the procedure below.

2.5 If an individual is uncertain about how this policy might affect his or her activities or has any questions about its application, he or she should contact the Law Department.

3. Conflict of Interest

3.1 What is a conflict of interest?

3.1.1 A conflict of interest is any situation in which a trustee's personal interests or loyalties could, or could be seen to, prevent the trustee from making a decision only in the best interests of the congregation.

3.1.2 A conflict of interest arises when the interests of a trustee (or a person closely connected to them, whether by family or business) are incompatible or in competition with the interests of the congregation. Such situations present a risk that trustees will make a decision based on external influences and that such a decision will not be in the best interests of the congregation.

The most common types of conflict include:

direct financial interest – where there is, or appears to be, an opportunity for personal financial gain

indirect financial interest – the financial gain of a close relative or close friend or business associate

The level of financial interest should not be a determining factor in deciding whether a conflict should be disclosed. The congregation expects disclosure of any financial interest, however small.

non-financial or personal conflicts - a non-financial interest can take many forms and is generally one where there is, or appears to be, an opportunity for personal benefit, advantage or enhancement to prospects for the individual (direct), or similar gains to someone in their immediate family or a person with whom the individual has a close personal relationship (indirect)

Conflicts of loyalties – a particular type of conflict of interest in which a trustee's loyalty or duty to another person or organisation could prevent the trustee from making a decision only in the best interests of the congregation.

3.1.3 A conflict of loyalty may arise where a trustee is also a charity trustee or member of another body (such as, for example, a local community group) if that could (or could be seen to) interfere with their ability to make decisions only in the best interests of the congregation. In such circumstances, a trustee must act at all times only in the best interests of the congregation in carrying out their trustee role, regardless of how decisions made in that role may impact on the other body.

3.1.4 The interests of the congregation will for the most part be consistent, or complementary, but it is inevitable that on occasion a conflict will arise. Whether a conflict of loyalty is of such low risk that the affected trustee can participate in the decision is a judgement for the trustees and will depend on the particular decision and circumstances of the case. It will often be the case that the potential damage that could be caused by any conflict is so minimal that it can be managed without any difficulty. The trustees must take all relevant factors into account and be ready to explain their approach if asked to do so.

3.2 Recognising and disclosing conflicts of interest

3.2.1 All trustees are required to recognise and disclose activities that might give rise to conflicts of interest, or the perception of conflicts of interest, at the earliest opportunity. This allows the other trustees to consider the issue of the conflict of interest to ensure that any potential effect on decision-making is eliminated and to demonstrate that their decision was made only in the best interests of the congregation. If properly managed, activities can proceed as normal whilst at the same time upholding the trustees' obligations to the congregation, meeting regulatory and other external requirements and protecting the integrity and reputation of the congregation. By contrast, conflicts which are not managed effectively may jeopardise the congregation's public standing and may cause serious damage to the reputation of the congregation and of the individuals concerned. It is therefore the congregation's policy to ensure that when conflicts or perceived conflicts of interest arise they are acknowledged and disclosed.

3.2.2 There can be situations in which the appearance of conflict of interest is present even when no conflict actually exists. It is important for all trustees when evaluating a potential conflict of interest to consider how it might be perceived by others. The duty to declare a possible conflict applies to the perception of the situation as much as to the actual existence of a conflict. When deciding whether such an interest is present, trustees should ask themselves whether a reasonable member of the public, with knowledge of all of the relevant facts of the situation, would think that their judgement might be prejudiced or influenced by their private or personal interest. This is an objective test. Trustees must not decide whether they would take a decision without prejudice, but whether they could be seen as doing so.

3.2.3 There may, exceptionally, be circumstances in which a conflict cannot be satisfactorily managed. In such circumstances the trustees should remove the conflict by not proceeding with a proposed course of action; by proceeding in a different way so that the conflict does not arise; or by not appointing a particular trustee or requiring the resignation of a trustee.

4. Procedure

4.1 It is the duty of every trustee to disclose any conflict of interest or any circumstances that might reasonably give rise to the perception of conflict of interest. The following procedure should be followed to ensure that conflicts of interest are identified at as early a stage as possible and that, once identified, action is taken to ensure that the conflict of

interest does not give rise to a situation where decisions are taken by trustees which are, or could be perceived as being, not in the best interests of the congregation.

4.2 Register of interests

4.2.1 New trustees will be informed before they are appointed that they will be expected to adhere to this conflict of interest policy and a copy of the policy will be provided to them. Any potential conflict of interest should be discussed with the Session Clerk prior to taking up the position.

4.2.2 On appointment, trustees will be required to complete a Declaration of Interests form (Appendix 1). A Register of Interests will be maintained by the Session Clerk and updated when a material change occurs. The Register of Interests must be reviewed and updated on an annual basis.

4.2.3 A copy of the policy will be provided to all current trustees, who will also be required to complete a Declaration of Interests form.

4.3 Disclosure

4.3.1 Any failure to disclose a potential, actual or perceived conflict of interest is a serious issue. A trustee who fails to disclose a potential, actual or perceived conflict will have failed to comply with their statutory duty.

4.3.2 There should be a standard agenda item at the beginning of each Kirk Session [and Congregational Board/Deacons' Court] meeting to declare any potential, actual or perceived conflicts of interest.

4.3.3 A trustee should declare any interest which he or she has in an item to be discussed, at the earliest possible opportunity and before any discussion of the item itself. If a trustee is uncertain whether he or she is conflicted he or she should err on the side of openness, declaring the issue and discussing it with the other trustees.

4.3.4 If a trustee is aware of an undeclared conflict of interest affecting another trustee they should notify the other trustees or the Chair. All trustees have a collective responsibility to manage conflicts and to act clearly in the congregation's best interests.

4.4 Managing conflicts of interest

4.4.1 If a potential, actual or perceived conflict of interest is identified the trustees must act only in the best interests of the congregation. This means the trustees must consider the issue of the conflict of interest so that any effect this may have on good decision-making is eliminated.

4.4.2 In deciding whether a conflict of interest exists trustees must consider the following:

Has the decision been taken in the best interests of the congregation?

Does the decision protect the reputation of the congregation?

What impression does the decision have on those outside the congregation?

Can the trustees demonstrate that they have made the decision in the best interests of the congregation and independently of any competing interests?

Does the presence of a conflicted trustee inhibit free discussion and influence the decisionmaking process in any way?

4.4.3 Where the trustees decide that there is a potential, actual or perceived conflict of interest the conflicted trustee should not participate in the decision-making process.

4.4.4 The conflicted trustee should withdraw from the meeting prior to discussion of the item.

4.4.5 The conflicted trustee should be given the opportunity before withdrawing from the meeting to provide any information necessary to help the remaining trustees make a decision in the best interests of the congregation.

4.4.6 A conflicted trustee should not take part in any vote on the item which is the subject of the conflict.

4.5 Recording

4.5.1 In all instances where a potential, actual or perceived conflict of interest is disclosed at a trustees' meeting the minutes of the meeting should record the trustees' discussion and the decision taken.

4.5.2 If there is a discussion, the written record of the decision should include:
the nature of the conflict which trustees were affected
whether any conflicts of interest were declared in advance
an outline of the discussion whether anyone withdrew
from the discussion
how the decision was taken in the best interests of the congregation

5 Consequences of breach

5.1 Where conflicts of interest are not identified or properly managed there can be serious consequences for both the affected trustee and the congregation. Decisions taken may not be valid and could be challenged and can damage the reputation of the congregation and the trust of the public.

5.2 If the circumstances are sufficiently serious, a failure to disclose a conflict of interest could therefore result in a disciplinary process being engaged.

6 Review

6.1 This Policy will be reviewed by the congregation after one year and thereafter every three years.

APPENDIX 1

REGISTER OF CHARITY TRUSTEES' INTERESTS

1. CONFLICTS POLICY

The charity trustees of [INSERT NAME OF CONGREGATION] have implemented a conflicts of interest policy under which they have agreed that a register will be kept of all interests declared by the charity trustees.

2. MAINTENANCE OF REGISTER

This register is maintained by the Session Clerk, who must:

record all conflicts, gifts and hospitality declared by the trustees in accordance with the policy; and circulate amendments or additions to the register (if any) to the trustees at the start of each charity trustee meeting.

3. REVIEWING THE REGISTER

As agreed in the policy, at least once in every 12-month period, all charity trustees must review the information relating to themselves contained in this register and declare that the information is correct or make a further declaration if necessary.

4. INSPECTION OF REGISTER

This register is available for inspection by any charity trustee and by any member of the congregation on request.

REGISTER OF INTERESTS

Date notified	Name of charity trustee	Brief details of interest notified	Brief details of any action taken