Non-Subscribing Presbyterian Church of Ireland

Data Protection Policy

CONTENTS

As adopted at the Pro Renata General Synod 31st January 2026.

1. Interpretation

1.1 Definitions:

Automated Decision-Making (ADM): when a decision is made which is based solely on Automated Processing (including profiling) which produces legal effects or significantly affects an individual. The UK GDPR prohibits Automated Decision-Making (unless certain conditions are met) but not Automated Processing.

Automated Processing: any form of automated processing of Personal Data consisting of the use of Personal Data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Profiling is an example of Automated Processing, as are many uses of artificial intelligence (AI) where they involve the processing of Personal Data.

Personnel: all employees, workers, contractors, agency workers, consultants, directors, members and others.

Consent: agreement which must be freely given, specific, informed and be an unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear positive action, signify agreement to the Processing of Personal Data relating to them.

Controller: the person or organisation that determines when, why and how to process Personal Data. It is responsible for establishing practices and policies in line with the UK GDPR. We are the Controller of all Personal Data relating to our Denomination Personnel and Personal Data used in our business for our own commercial purposes.

Criminal Convictions Data: personal data relating to criminal convictions and offences, including personal data relating to criminal allegations and proceedings.

Data Subject: a living, identified or identifiable individual about whom we hold Personal Data. Data Subjects may be nationals or residents of any country and may have legal rights regarding their Personal Data.

Data Privacy Impact Assessment (DPIA): tools and assessments used to identify and reduce risks of a data processing activity. A DPIA can be carried out as part of Privacy by Design and should be conducted for all major system or business change programmes involving the Processing of Personal Data.

Data Protection Officer (DPO): either of the following:

a) the person required to be appointed in specific circumstances under the UK GDPR; or

b) where a mandatory DPO has not been appointed, a data privacy manager or other voluntary appointment of a DPO or the Church data privacy team with responsibility for data protection compliance.

Explicit Consent: consent which requires a very clear and specific statement (that is, not just action).

UK GDPR: the retained EU law version of the General Data Protection Regulation (*(EU) 2016/679*) as defined in the Data Protection Act 2018. Personal Data is subject to the legal safeguards specified in the UK GDPR.

Personal Data: any information identifying a Data Subject or information relating to a Data Subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. Personal Data includes Special Categories of Personal Data and Pseudonymised Personal Data but excludes anonymous data or data that has had the identity of

an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

Personal Data means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Personal Data Breach: any act or omission that compromises the security, confidentiality, integrity or availability of Personal Data or the physical, technical, administrative or organisational safeguards that we or our third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of Personal Data is a Personal Data Breach.

Privacy by Design: implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the UK GDPR. The UK GDPR requires you to put in place appropriate technical and organisational measures to implement the data protection principles effectively and safeguard individual rights. This is 'data protection by design and by default'.

Privacy Notices (also referred to as Fair Processing Notices) or Privacy Policies: separate notices setting out information that may be provided to Data Subjects when the Church collects information about them. These notices may take the form of:

a) general privacy statements applicable to a specific group of individuals (for example, employee privacy notices or the website privacy policy); or

b) stand-alone, one-time privacy statements covering Processing related to a specific purpose.

Processing or Process: any activity that involves the use of Personal Data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring Personal Data to third parties.

Pseudonymisation or Pseudonymised: replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person to whom the data relates cannot be identified without the use of additional information which is meant to be kept separately and secure.

Special Categories of Personal Data: information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data.

2. Introduction

2.1 This Data Protection Policy sets out how the Non-Subscribing Presbyterian Church in Ireland (NSPCI) ("we", "our", "us", "the Church") handle the Personal Data of our members, prospective members, suppliers, employees, workers, business contacts and other third parties.

2.2 This Data Protection Policy applies to all Personal Data we Process regardless of the media on which that data is stored or whether it relates to past or present employees, workers, members, clients or supplier contacts, shareholders, website users, or any other Data Subject.

2.3 This Data Protection Policy applies to all Denomination Personnel ("you", "your"). You must read, understand and comply with this Data Protection Policy when Processing Personal Data on our behalf and attend training on its requirements. Data protection is the responsibility of everyone within the Church and this Data Protection Policy sets out what we expect from you when handling Personal Data to enable the Church to comply with applicable law. Your compliance with this Data Protection Policy is mandatory. Related Policies and Privacy Guidelines are available to help you interpret and act in accordance with this Data Protection Policy. You must also comply with all those Related Policies and Privacy Guidelines. Any breach of this Data Protection Policy may result in disciplinary action.

2.4 Where you have a specific responsibility in connection with Processing, such as capturing Consent, reporting a Personal Data Breach or conducting a DPIA as referenced in this Data Protection Policy or otherwise, then you must comply with the Related Policies and Privacy Guidelines.

2.5 This Data Protection Policy (together with Related Policies and Privacy Guidelines) is an internal document and cannot be shared with third parties, clients or regulators without prior authorisation from the DPO.

3. Scope of Policy and when to seek advice on data protection compliance

3.1 We recognise that the correct and lawful treatment of Personal Data will maintain trust and confidence in the organisation and will provide for successful business operations. Protecting the confidentiality and integrity of Personal Data is a critical responsibility that we take seriously at all times. The Church is exposed to potential fines of up to £17.5 million or 4% of total worldwide annual turnover, whichever is higher and depending on the breach, for failure to comply with the UK GDPR.

3.2 All members of the Clergy, laity as well as employees are responsible for ensuring all Denomination Personnel comply with this Data Protection Policy and need to implement appropriate practices, processes, controls and training to ensure that compliance.

3.3 The DPO is responsible for overseeing this Data Protection Policy and, as applicable, developing Related Policies and Privacy Guidelines. That post is held by [NAME], and they can be reached at [TELEPHONE NUMBER] and [EMAIL ADDRESS].

3.4 Please contact the DPO with any questions about the operation of this Data Protection Policy or the UK GDPR or if you have any concerns that this Data Protection Policy is not being or has not been followed. In particular, you should contact the DPO in the following circumstances:

(a) if you are unsure of the lawful basis on which you are relying to process Personal Data (including the legitimate interests used by the Church) (see paragraph 5.1);

(b) if you need to rely on Consent or need to capture Explicit Consent (see paragraph 5.11);

(c) if you need to draft Privacy Notices (see paragraph 6); see appendix 3

(d) if you are unsure about the retention period for the Personal Data being Processed (see paragraph 10);

(e) if you are unsure what security or other measures you need to implement to protect Personal Data (see paragraph 11.1);

(f) if there has been a Personal Data Breach (paragraph 12);

(g) if you are unsure on what basis to transfer Personal Data outside the UK (see paragraph 13);

(h) if you need any assistance dealing with any rights invoked by a Data Subject or complaints (see paragraph 14);

(i) whenever you are engaging in a significant new, or change in, Processing activity which is likely to require a DPIA (see paragraph 18) or plan to use Personal Data for purposes other than for which it was collected (see paragraph 7);

(j) if you plan to undertake any activities involving Automated Processing including profiling or Automated Decision-Making (see paragraph 19);

(k) if you need help complying with applicable law when carrying out direct marketing activities (see **Error! Bookmark not defined.Error! Reference source not found.**); or

(l) if you need help with any contracts or other areas in relation to sharing Personal Data with third parties (including our vendors) (see paragraph 20).

4. Personal data protection principles

4.1 We adhere to the principles relating to Processing of Personal Data set out in the UK GDPR which require Personal Data to be:

(a) Processed lawfully, fairly and in a transparent manner (lawfulness, fairness and transparency);

(b) collected only for specified, explicit and legitimate purposes (purpose limitation);

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed (data minimisation);

(d) accurate and where necessary kept up to date (accuracy);

(e) not kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the data is Processed (storage limitation);

(f) Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful Processing and against accidental loss, destruction or damage (security, integrity and confidentiality);

(g) not transferred to another country without appropriate safeguards in place (transfer limitation); and

(h) made available to Data Subjects and allow Data Subjects to exercise certain rights in relation to their Personal Data (data subject's rights and requests).

4.2 We are responsible for and must be able to demonstrate compliance with the data protection principles listed above (accountability).

5. Lawfulness, fairness and transparency

5.1 Personal data must be Processed lawfully, fairly and in a transparent manner in relation to the Data Subject.

5.2 You may only collect, Process and share Personal Data fairly and lawfully and for specified purposes. The UK GDPR restricts our actions regarding Personal Data to specified lawful purposes. These restrictions are not intended to prevent Processing but ensure that we Process Personal Data fairly and without adversely affecting the Data Subject.

5.3 The UK GDPR allows Processing for specific purposes, some of which are set out below:

(a) the Data Subject has given their Consent;

(b) the Processing is necessary for the performance of a contract with the Data Subject;

(c) to meet our legal compliance obligations;

(d) to protect the Data Subject's vital interests;

(e) to pursue our legitimate interests (or those of a third party) for purposes where they are not overridden because the Processing prejudices the interests or fundamental rights and freedoms of Data Subjects. The purposes for which we process Personal Data for legitimate interests need to be set out in applicable Privacy Notices; or

5.4 You must identify and document the legal ground being relied on for each Processing activity**.**

(a) What are the lawful bases for processing?

5.5 (a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose.

5.6 (b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

5.7 (c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).

5.8 (d) Vital interests: the processing is necessary to protect someone's life.

5.9 (e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

5.10 (f) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

5.11 Consent

5.12 A Controller must only process Personal Data on one or more of the lawful bases set out in the UK GDPR, which include Consent.

5.13 A Data Subject consents to Processing of their Personal Data if they clearly indicate agreement to the Processing. Consent requires affirmative action, so silence, pre-ticked boxes or inactivity will not be sufficient to indicate consent. If Consent is given in a document which deals with other matters, then the Consent must be kept separate from those other matters.

5.14 A Data Subject must be easily able to withdraw Consent to Processing at any time and withdrawal must be promptly honoured. Consent may need to be refreshed if you intend to Process Personal Data for a different and incompatible purpose which was not disclosed when the Data Subject first consented.

5.15 When processing Special Category Data or Criminal Convictions Data, we will usually rely on a legal basis for processing other than Explicit Consent or Consent if possible. Where Explicit Consent is relied on, you must issue a Privacy Notice to the Data Subject to capture Explicit Consent.

5.16 You will need to evidence Consent captured and keep records of all Consents in accordance with Related Policies and Privacy Guidelines, so that the Church can demonstrate compliance with Consent requirements.

6. Transparency (notifying Data Subjects)

6.1 The UK GDPR requires a Controller to provide detailed, specific information to a Data Subject depending on whether the information was collected directly from the Data Subject or from elsewhere. The information must be provided through an appropriate Privacy Notice which must be concise, transparent, intelligible, easily accessible, and in clear and plain language so that a Data Subject can easily understand them.

6.2 Whenever we collect Personal Data directly from a Data Subject, including for HR or employment purposes, we must provide the Data Subject with all the information required by the UK GDPR including the identity of the Controller and DPO, and how and why we will use, Process, disclose, protect and retain that Personal Data through a Privacy Notice which must be presented when the Data Subject first provides the Personal Data.

6.3 When Personal Data is collected indirectly (for example, from a third party or publicly available source), we must provide the Data Subject with all the information required by the UK GDPR as soon as possible after collecting or receiving the data. We must also check that the Personal Data was collected by the third party in accordance with the UK GDPR and on a basis which contemplates our proposed Processing of that Personal Data.

6.4 If you are collecting Personal Data from a Data Subject, directly or indirectly, then you must provide the Data Subject with a Privacy Notice in accordance with our Related Policies and Privacy Guidelines.

6.5 You must comply with the Church's guidelines on Privacy.

7. Purpose limitation

7.1 Personal Data must be collected only for specified, explicit and legitimate purposes. It must not be further Processed in any manner incompatible with those purposes.

7.2 You cannot use Personal Data for new, different or incompatible purposes from that disclosed when it was first obtained unless you have informed the Data Subject of the new purposes and they have Consented where necessary.

7.3 If you want to use Personal Data for a new or different purpose from that for which it was obtained, you must first contact the DPO for advice on how to do this in compliance with both the law and this Data Protection Policy.

8. Data minimisation

8.1 Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed.

8.2 You may only Process Personal Data when performing your duties requires it. You cannot Process Personal Data for any reason unrelated to your duties.

8.3 You may only collect Personal Data that you require for your duties: do not collect excessive data. Ensure any Personal Data collected is adequate and relevant for the intended purposes.

8.4 You must ensure that when Personal Data is no longer needed for specified purposes, it is deleted or anonymised in accordance with the Church's data retention guidelines.

9. Accuracy

9.1 Personal Data must be accurate and, where necessary, kept up to date. It must be corrected or deleted without delay when inaccurate.

9.2 You must ensure that the Personal Data we use and hold is accurate, complete, kept up to date and relevant to the purpose for which we collected it. You must check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards. You must take all reasonable steps to destroy or amend inaccurate or out-of-date Personal Data.

10. Storage limitation

10.1 Personal Data must not be kept in an identifiable form for longer than is necessary for the purposes for which the data is processed.

10.2 The Church will maintain retention policies and procedures to ensure Personal Data is deleted after an appropriate time, unless a law requires that data to be kept for a minimum time. [

10.3 You must not keep Personal Data in a form which permits the identification of the Data Subject for longer than needed for the legitimate business purpose or purposes for which we originally collected it including for the purpose of satisfying any legal, accounting or reporting requirements.

10.4 You will take all reasonable steps to destroy or erase from our systems all Personal Data that we no longer require in accordance with all the Church's applicable records retention schedules and policies. This includes requiring third parties to delete that data where applicable.

10.5 You will ensure Data Subjects are provided with information about the period for which data is stored and how that period is determined in any applicable Privacy Notice.

11. Security integrity and confidentiality

11.1 Personal Data must be secured by appropriate technical and organisational measures against unauthorised or unlawful Processing, and against accidental loss, destruction or damage.

11.2 We will develop, implement and maintain safeguards appropriate to our size, scope and business, our available resources, the amount of Personal Data that we own or maintain on behalf of others, and identified risks (including use of encryption and Pseudonymisation where applicable). We will regularly evaluate and test the effectiveness of those safeguards to ensure security of our Processing of Personal Data. You are responsible for protecting the Personal Data we hold. You must implement reasonable and appropriate security measures against unlawful or unauthorised Processing of Personal Data and against the accidental loss of, or damage to, Personal Data. You must exercise particular care in protecting Special Categories of Personal Data and Criminal Convictions Data from loss and unauthorised access, use or disclosure.

11.3 You must follow all procedures and technologies we put in place to maintain the security of all Personal Data from the point of collection to the point of destruction. You may only transfer Personal Data to third-party service providers who agree to comply with the required policies and procedures and who agree to put adequate measures in place, as requested.

11.4 You must maintain data security by protecting the confidentiality, integrity and availability of the Personal Data, defined as follows:

(a) Confidentiality: only people who have a need to know and are authorised to use the Personal Data can access it;

(b) Integrity: Personal Data is accurate and suitable for the purpose for which it is processed; and

(c) Availability: authorised users are able to access the Personal Data when they need it for authorised purposes.

11.5 You must comply with and not attempt to circumvent the administrative, physical and technical safeguards we implement and maintain in accordance with the UK GDPR and relevant standards to protect Personal Data.

12. Reporting a Personal Data Breach

12.1 The UK GDPR requires Controllers to notify any Personal Data Breach to the Information Commissioner and, in certain instances, the Data Subject.

12.2 We have put in place procedures to deal with any suspected Personal Data Breach and will notify the Data Subject or any applicable regulator where we are legally required to do so.

12.3 If you know or suspect that a Personal Data Breach has occurred, do not attempt to investigate the matter yourself. Immediately contact the Data Protection Lead for the respective church body as the key point of contact for Personal Data Breaches.

13. Transfer limitation

13.1 The UK GDPR restricts data transfers to countries outside the UK to ensure that the level of data protection afforded to individuals by the UK GDPR is not undermined. You transfer Personal Data originating in one country across borders when you transmit, send, view or access that data in or to a different country.

13.2 You may only transfer Personal Data outside the UK if one of the following conditions applies:

(a) the UK has issued regulations confirming that the country to which we transfer the Personal Data ensures an adequate level of protection for the Data Subject's rights and freedoms;

(b) appropriate safeguards are in place such as binding corporate rules, standard contractual clauses approved for use in the UK, an approved code of conduct or a certification mechanism, a copy of which can be obtained from the DPO;

(c) the Data Subject has provided Explicit Consent to the proposed transfer after being informed of any potential risks; or

(d) the transfer is necessary for one of the other reasons set out in the UK GDPR including:

(i) the performance of a contract between us and the Data Subject;

(ii) reasons of public interest;

(iii) to establish, exercise or defend legal claims;

(iv) to protect the vital interests of the Data Subject where the Data Subject is physically or legally incapable of giving Consent; and

(v) in some limited cases, for our legitimate interest.

14. Data Subject's rights and requests

14.1 A Data Subject has rights when it comes to how we handle their Personal Data. These include rights to:

(a) withdraw Consent to Processing at any time;

(b) receive certain information about the Controller's Processing activities;

(c) request access to their Personal Data that we hold (including receiving a copy of their Personal Data);

(d) prevent our use of their Personal Data for direct marketing purposes;

(e) ask us to erase Personal Data if it is no longer necessary in relation to the purposes for which it was collected or Processed or to rectify inaccurate data or to complete incomplete data;

(f) restrict Processing in specific circumstances;

(g) object to Processing which has been justified on the basis of our legitimate interests or in the public interest;

(h) request a copy of an agreement under which Personal Data is transferred outside of the UK;

(i) object to decisions based solely on Automated Processing, including profiling (ADM);

(j) prevent Processing that is likely to cause damage or distress to the Data Subject or anyone else;

(k) be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms;

(l) make a complaint to us and subsequently to the supervisory authority;

(m) in limited circumstances, receive or ask for their Personal Data to be transferred to a third party in a structured, commonly used and machine-readable format; and

14.2 You must verify the identity of an individual requesting data under any of the rights listed above (do not allow third parties to persuade you into disclosing Personal Data without proper authorisation).

14.3 You must immediately forward any Data Subject request or complaint you receive to the Data Protection Lead for the relevant church body.

15. Accountability

15.1 The Controller must implement appropriate technical and organisational measures in an effective manner to ensure compliance with data protection principles. The Controller is responsible for, and must be able to demonstrate, compliance with the data protection principles.

15.2 The Church must have adequate resources and controls in place to ensure and to document UK GDPR compliance including:

(a) appointing a suitably qualified DPL (where necessary) and an GPC member accountable for data privacy;

(b) implementing Privacy by Design when Processing Personal Data and completing DPIAs where Processing presents a high risk to rights and freedoms of Data Subjects;

(c) integrating data protection into internal documents including this Data Protection Policy, Related Policies, Privacy Guidelines or Privacy Notices;

(d) regularly training Denominational Personnel on the UK GDPR, this Data Protection Policy, Related Policies and Privacy Guidelines, and data protection matters including, for example, a Data Subject's rights, Consent, legal basis, DPIA and Personal Data Breaches. The Church must maintain a record of training attendance by Denominational Personnel; and

(e) regularly testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance, including using results of testing to demonstrate compliance improvement effort.

16. Record keeping

16.1 The UK GDPR requires us to keep full and accurate records of all our data Processing activities.

16.2 You must keep and maintain accurate corporate records reflecting our Processing including records of Data Subjects' Consents and procedures for obtaining Consents [in accordance with the Church's record-keeping guidelines].

16.3 These records should include, at a minimum:

(a) the name and contact details of the Controller and the DPO; and

(b) clear descriptions of:

(i) the Personal Data types;

(ii) the Data Subject types;

(iii) the Processing activities;

(iv) the Processing purposes;

(v) the third-party recipients of the Personal Data;

(vi) the Personal Data storage locations;

(vii) the Personal Data transfers;

(viii) the Personal Data's retention period; and

(ix) the security measures in place.

16.4 To create the records, data maps should be created which should include the detail set out above together with appropriate data flows, [in accordance with the Church's record-keeping guidelines].

17. Training and audit

17.1 We are required to ensure all Denominational Personnel have undergone adequate training to enable them to comply with data privacy laws. We must also regularly test our systems and processes to assess compliance.

17.2 You must undergo all mandatory data privacy-related training and ensure your team undergoes similar mandatory training.

17.3 You must regularly review all the systems and processes under your control to ensure they comply with this Data Protection Policy and check that adequate governance controls and resources are in place to ensure proper use and protection of Personal Data.

18. Privacy by Design and Data Protection Impact Assessment (DPIA)

18.1 We are required to implement Privacy by Design measures when Processing Personal Data by implementing appropriate technical and organisational measures (like Pseudonymisation) in an effective manner, to ensure compliance with data privacy principles.

18.2 You must assess what Privacy by Design measures can be implemented on all programmes, systems or processes that Process Personal Data by taking into account the following:

(a) The state of the art.

(b) The cost of implementation.

(c) The nature, scope, context and purposes of Processing.

(d) The risks of varying likelihood and severity for rights and freedoms of the Data Subject posed by the Processing.

18.3 The Controller must also conduct a DPIA in respect to high-risk Processing.

18.4 You should conduct a DPIA (and discuss your findings with the DPO) when implementing major system or business change programs involving the Processing of Personal Data including:

(a) Use of new technologies (programs, systems or processes, including the use of AI), or changing technologies (programs, systems or processes).

(b) Automated Processing including profiling and ADM.

(c) Large-scale Processing of Special Categories of Personal Data or Criminal Convictions Data.

(d) Large-scale, systematic monitoring of a publicly accessible area.

18.5 A DPIA must include:

(a) A description of the Processing, its purposes and the Controller's legitimate interests if appropriate.

(b) An assessment of the necessity and proportionality of the Processing in relation to its purpose.

(c) An assessment of the risk to individuals.

(d) The risk mitigation measures in place and demonstration of compliance.

19. Automated Processing (including profiling) and Automated Decision-Making

19.1 Generally, ADM is prohibited when a decision has a legal or similar significant effect on an individual unless:

(a) a Data Subject has Explicitly Consented;

(b) the Processing is authorised by law; or

(c) the Processing is necessary for the performance of or entering into a contract.

19.2 If certain types of Special Categories of Personal Data or Criminal Convictions Data are being processed, then grounds (b) or (c) will not be allowed. However, the Special Categories of Personal Data and Criminal Convictions Data can be Processed where it is necessary (unless less intrusive means can be used) for substantial public interest like fraud prevention.

19.3 If a decision is to be based solely on Automated Processing (including profiling), then the Data Subject must be informed when you first communicate with them of their right to object. This right must be explicitly brought to their attention and presented clearly and separately from other information. Further, suitable measures must be put in place to safeguard the Data Subject's rights and freedoms and legitimate interests.

19.4 We must also inform the Data Subject of the logic involved in the decision making or profiling, the significance and the envisaged consequences, and give the Data Subject the right to request human intervention, express their point of view or challenge the decision.

19.5 A DPIA must be carried out before any Automated Processing (including profiling) or ADM activities are undertaken.

19.6 [Where you are involved in any data Processing activity that involves profiling or ADM, you must comply with the Church's guidelines on profiling or ADM.]

20. Sharing Personal Data

20.1 Generally, we are not allowed to share Personal Data with third parties unless certain safeguards and contractual arrangements have been put in place.

20.2 You must comply with the Church's guidelines on sharing data with third parties.

20.3 You may only share the Personal Data we hold with another employee, agent or representative of our Denomination if the recipient has a need to know the information and the transfer complies with any applicable cross-border transfer restrictions.

20.4 You may only share the Personal Data we hold with third parties, such as our service providers, if:

(a) they have a need to know the information for the purposes of providing the contracted services;

(b) sharing the Personal Data complies with the Privacy Notice provided to the Data Subject and, if required, the Data Subject's Consent has been obtained;

(c) the third party has agreed to comply with the required data security standards, policies and procedures, and put adequate security measures in place;

(d) the transfer complies with any applicable cross-border transfer restrictions; and

(e) a fully executed written contract that contains UK GDPR-compliant third party clauses has been obtained.

21. Changes to this Data Protection Policy

21.1 This policy will be reviewed bi-annually by the General Purposes Committee..

21.2 This Data Protection Policy does not override any applicable national data privacy laws and regulations in countries where the Church operates.

Appendix 1 Hints and Tips — Good Data Protection Practice*

• Respect everyone's privacy.

• Data should only be used and stored electronically for Church matters, administration and the specific purpose the information was collected for: not shared without permission outside the Church.

• Ensure that paper records are kept in a locked cupboard.

• Do not disclose any personal information about an individual without first obtaining that person's consent—that includes, address, telephone number, email address, age, birthday, names of family members.'

• Consider data security when sending e-mails regarding Church matters from a personal email address. You may wish to set up a congregational or office bearer email addresses using a provider like Mircrosoft outlook e.g. ***secretary.congregation@outlook.com*** or ***congregation.nspci@outlook.com***

• When emailing groups of people always put their email addresses In the 'bcc' row rather than the 'To' row. This prevents an individual's email address being visible to all the recipients

• If you are sharing birthday information (age or date) about an individual with others always ask for the individual's permission first. Ideally this should be in writing.

• When mentioning pastoral concerns or praying for identifiable individuals take reasonable steps to ensure that the individual (and anyone else who may be directly or indirectly involved) is willing for this to happen.

• When minuting pastoral concerns, refrain from mentioning names and the nature of the concern.

• Prayer lists should be confidentially destroyed immediately after they have been used.

Personal data held on laptops, data sticks and other portable electronic devices should be encrypted. If data is held in electronic form then the Congregation may need to register with the ICO.

• If using cloud storage ensure that the servers are located within the European Economic

Area (PEA) and take reasonable steps to ensure security.

• When collecting an e-mail always ask for consent from the owner of the e-mail: do not assume consent if the e-mail address is supplied by a third party. e.g "*These e-mail addresses will only be used for issues related to Congregation for purpose of …… This information will not be shared with third parties. Should you wish to remove your email address from this list please let us know*"

• Order your records —minimise what you keep.

• Check that existing and former officers/elders/committee members are not retaining their own copies of personal data in paper form or electronically. Seek their confirmation that all such data has been returned or destroyed

*Based on information produced by United Reformed Church, Hints and tips Good Data Protection Practice vl - I February 2015

Appendix 2 - Establishing Good Data Protection Practice in Your Church Checklist*

REMEMBER - Data Protection legislation applies to both paper and electronic records and includes photos and videos as well as documents.

1. Confirm who is the Data Controller for each of the various church bodies ie General Synod, Committees, Presbytery and congregations.

2. Make sure that the Data Controller(s) understands what constitutes personal data.

(Personal data relates to a living individual who can be identified from that data.

Identification can be by the information alone or in conjunction with any other

information in the data controller's possession or likely to come into such possession.)

3. Make sure that the Data Controller(s) understand what constitutes SPECIAL CATEGORY

(sensitive) personal data (ie data which contains information about: racial/ethnic origin;

political opinions; religious or philosophical beliefs; TU membership; genetic/biometric

for identification; health; sex life and sexual orientation. Special Category data can only

be processed with explicit consent.

4. Compile a full list of all the types of personal data each of the various church bodies ie General Synod, Committees, Presbytery and congregations collects and holds.

5. For each type of information determine where and how it Is held.

6. Ensure that the data is held securely. Take steps to ensure that personal data is not

disclosed to others without that person's permission — this includes: birthdays;

addresses; telephone numbers; email addresses; matters relating a person's health.

7. For each type of information determine how long it should be held and be able to justify

your decisions.

8. Dispose securely of any data which is no longer useful.

9. For each type of information establish a routine for the permanent and secure disposal

of time-expired data.

10. Determine who will deal with Subject Access Requests (SAR). Usually the Church

Secretary.

11. Make sure that the Church Secretary or other relevant person(s) know that there is a

statutory limit (30 days) within which to comply with a Subject Access Request.

12. Complete and publish your congregations Privacy notice (you may amend the Denominational Privacy statement in the appendix 3).

13. Make sure that the Privacy Notice is posted in a prominent position and that

members, friends and adherents are aware of its existence and that copies are available

for them to take away.

14. Bring the Privacy notice to the notice of members at a Church Meeting and review

regularly its effectiveness - suggest at Annual Church Meeting.

15. Monitor, review and amend as necessary.

*The United Reformed Church, GDPR Checklist vi —1 February 2018

Appendix 3

The purpose of this privacy notice

The Non-Subscribing Presbyterian Church in Ireland (NSPCI) is committed to protecting the privacy and security of your personal information (referred to as **personal data**) and is required by data protection law to provide you with this privacy notice.

This notice applies to members, prospective members, office bearers, visitors, clergy, employees, workers, consultants and contractors. It does not form part of any contract of employment, contract of service or contract to provide services.

Read and retain this notice so that you understand how we collect, store and use your personal data during and after your association with us and so that you are aware of your rights under data protection law. A copy of the notice is also available from nspresbyterian.org

We may update this notice at any time. If we do, we will provide you with an updated copy, summarising the changes where relevant. We may also notify you in other ways from time to time about the processing of your personal data.

You should ensure that you are familiar with our Data Protection Policy.

Who we collect your personal data from

We collect personal data about members, prospective members, office bearers, visitors, clergy, employees, workers, consultants and contractors through our various processes, either directly from you or sometimes from third parties such as recruitment agencies, background check providers and referees.

We may also collect personal data from our clergy and congregations when circulating information about the events or the NSPCI.

We may sometimes collect additional data from third parties including former employers, credit reference agencies and HMRC and Charity Commission.

We may also collect personal data from the trustees or managers of pension arrangements operated by us.

We may collect additional personal data during the course of your association with us. Where necessary, we will provide a further privacy notice to you about the source of that data and what we are doing with it.

The types of personal data we hold about you

Personal data means any information about an individual from which that person can be identified. It does not include information from which the person's identity has been removed (anonymous data).

There are certain types of personal data that reveal more sensitive personal details, such as health information or criminal convictions. Special category data and criminal offence data are treated with additional care and are addressed separately in this notice.

If any of the following information changes, contact The Clerk of the General Synod so that we can ensure that all the information we hold about you is accurate and up to date.

We may collect, store and use the following categories of **personal data** about you depending on whether you are a members, prospective members, office bearers, visitors, clergy, employees, workers, consultants and contractors and what the requirements of this information maybe:

- **Identity data:** first name, last name, any previous names, marital status, title, date of birth and gender.
- **Contact data:** addresses, telephone numbers, personal email addresses and emergency contact information.
- **Family data:** dependants and next of kin.
- **Recruitment data:** copies of right to work documentation, copy passport or other photo ID, copy proof of address documentation (for example, bank statement or utility bill), copy driving licence, references and information included in a CV or cover letter or as part of the application process.
- **Employment status check data:** results of HMRC employment status check and details of your interest in and connection with the intermediary through which your services are supplied.
- **Financial and tax data:** National Insurance number, bank account details, payroll records and tax status information, salary, pension and benefits information, compensation history and conflict of interest or gift declarations.
- **Employment data:** start date (and, if different, start date of continuous employment), location of employment or workplace, leaving date and reason for leaving, employment records (including contracts, photographs, job titles, work history, working hours, working arrangements (office-based, hybrid, remote), holidays and other types of leave, training records and professional memberships), performance information and disciplinary and grievance information.
- **Monitoring data:** CCTV footage, and information about your use of our information and communications systems should that be introduced.

We **may** collect, store and use the following **special category data**:

- **Race, religion, beliefs and sexual orientation:** information about your race or ethnicity, religious or philosophical beliefs, sexual orientation and political opinions.
- **Trade union membership**.
- **Health and medical:** information about and connected with your health, any medical condition or disability, including:
    - sickness absence records;
    - accident at work records;
    - tailored adjustment records; and
    - correspondence with and information provided to and received from our occupational health service and other medical health professionals.

We **may** collect, store and use **criminal offence data** about you. This is information about criminal convictions and offences, including information relating to the alleged commission of offences, proceedings for an offence committed (or alleged to have been committed) and the disposal of those proceedings, including sentencing.

How we use your personal data

We will only use your personal data when we have a lawful basis to do so. Our lawful basis for each purpose for which we use your personal data is set out below. Most commonly, we will use your personal data in reliance on:

- **Contract performance.** Where we need to process your personal data to perform the contract we have entered into with you.

- **Legitimate interests.** Where we need to use your personal data for our legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests. We consider any potential impact on you and your rights when determining whether we can process your personal data for our legitimate interests. You can obtain further information about how we assess our legitimate interests against any potential impact on you in respect of specific activities by contacting our Data Protection Lead (**DPL**).
- **Legal obligation.** Where we need to use your personal data to comply with a legal or regulatory obligation.

Less commonly, we may need to process your personal data in emergency situations when it is in your **vital interests** or those of another person. This list below will be reviewed as the policy beds down and we review the information held.

Human Resource matters

Purpose/Use	**Type of data**	**Lawful basis**
HR records: setting up your record in the Presbytery or Denomination. Right to work: confirming entitlement to work in the UK Employment status: determining whether your engagement is deemed employment for the purposes of Chapter 10 of Part 2 of the Income Tax (Earnings and Pensions) Act 2003 and providing you with a status determination statement in accordance with the applicable provisions of that Act	Identity data Contact data Family data Recruitment data Employment status check data Financial and tax data Employment data Monitoring data	Contract performance Legal obligation Our legitimate interests which are IDENTIFY Third party legitimate interests of THIRD PARTY which are IDENTIFY Vital interests

Managing your contractual entitlements (pay, pensions, other benefits and leave)

Purpose/Use	**Type of data**	**Lawful basis**
Pay: paying you and, where required, deducting tax and National Insurance contributions (**NICs**) Salary and compensation: making decisions in salary reviews and in relation to other forms of compensation Pension enrolment: enrolling you in our pension scheme **OR** a pension arrangement in accordance with our statutory automatic enrolment duties Pension arrangements: liaising with the trustees or managers of any pension scheme **OR** arrangement operated by us **OR** your pension provider Annual leave: administering your annual leave entitlement and your entitlement to any other	Identity data Contact data Family data Recruitment data Employment status check data Financial and tax data Employment data Monitoring data	Contract performance Legal obligation Our legitimate interests which are IDENTIFY Third party legitimate interests of THIRD PARTY which are IDENTIFY Vital interests

forms of leave whether provided by law or under the terms of your contract with us		

Managing our association with you

Purpose/Use	Type of data	Lawful basis
Contract, policies and procedures: administering the call we have entered into with you and the policies and procedures set out in our as they apply to you from time to time Qualifications and skills: assessing qualifications and skills for a particular job or task. Education, training and development requirements Performance: conducting performance reviews, managing performance and determining performance requirements Grievance and disciplinary: investigating and conducting proceedings in relation to grievance or disciplinary issues raised by or concerning you Working arrangements: making decisions about your working arrangements and your continued employment or engagement Termination: making arrangements for the termination of our working relationship Legal disputes: dealing with any legal disputes we have with you	Identity data Contact data Family data Recruitment data Employment status check data Financial and tax data Employment data Monitoring data	Contract performance Legal obligation Our legitimate interests which are IDENTIFY Third party legitimate interests of THIRD PARTY which are IDENTIFY Vital interests

Contact – Individual congregations will need to consider what personal data they hold and for what purpose.

Purpose/Use	Type of data	Lawful basis
To contact about denominational business, policy updates, call of meetings.	Identity data Contact data Family data Employment check data Financial and tax data Employment data Monitoring data	Our legitimate interests which are IDENTIFY Third party legitimate interests of THIRD PARTY which are IDENTIFY Vital interests

Monitoring

Purpose/Use	Type of data	Lawful basis
Network and information security: ensuring network and information security, including prevention of unauthorised access to our computer and electronic communications systems and prevention of malicious software distribution Communication systems: monitoring use of our information and communication systems to ensure compliance with our IT policies Physical access: monitoring and controlling access to office premises	Identity data Contact data Family data Recruitment data Employment status check data Financial and tax data Employment data Monitoring data	Contract performance Legal obligation Our legitimate interests which are IDENTIFY Third party legitimate interests of THIRD PARTY which are IDENTIFY Vital interests

Wider relationship management

Purpose/Use	Type of data	Lawful basis
Business management and planning: DETAILS, including accounting and auditing Equal opportunities monitoring Health and safety: compliance with health and safety obligations Incidents: dealing with accidents and emergencies Legal disputes: dealing with legal disputes involving employees, workers and contractors or clients, members and suppliers Fraud or Crime prevention	Identity data Contact data Family data Recruitment data Employment status check data Financial and tax data Employment data Monitoring data	Contract performance Legal obligation Our legitimate interests which are IDENTIFY Third party legitimate interests of THIRD PARTY which are IDENTIFY Vital interests

How we use your special category data

We only use your special category data when, in addition to having a lawful basis that is required to process personal data (referred to previously in this notice), there is an additional ground that permits us to do so. Those additional grounds include:

- **Employment law.** When using your special category data is necessary for carrying out rights and obligations in connection with employment law.
- **Legal claims.** When using your special category data is necessary for establishing, exercising or defending legal claims.
- **Substantial public interest.** When using your special category data is necessary to undertake matters deemed to be of substantial public interest. These include equal opportunities monitoring, preventing or detecting unlawful acts, protecting the public against dishonesty, compliance with regulatory requirements in relation to unlawful acts, provision of confidential counselling and in relation to our occupational pension scheme.

- **Assessment of working capacity.** When using your special category data is necessary for the assessment of your working capacity by a health professional. Inline with Sickness Management Policy, Equal Opportunities Policy, Disability Discrimination Policy.
- **Vital interests (incapacity).** When using your special category data is necessary to protect your vital interests, or someone else's vital interests, in circumstances in which you may be physically or legally incapable of giving consent.

Race or ethnicity, religious or philosophical beliefs, sexual orientation, political opinions

Purpose/Use	Lawful basis	Additional ground
Equal opportunities monitoring and reporting Disciplinary and grievances issues Legal disputes	Contract performance Legal obligation Our legitimate interests which are IDENTIFY Third party legitimate interests of THIRD PARTY which are IDENTIFY Vital interests	Employment law Legal claims Substantial public interest

Trade union membership

Purpose/Use	Lawful basis	Additional ground
• Payment of trade union subscriptions • Communications: with your trade union, its officials and representatives • Exercise of your rights: as a trade union member or trade union representative • Disciplinary and grievances issues • Industrial action • Employment law • Legal claims/Disputes	Contract performance Legal obligation Our legitimate interests which are IDENTIFY Third party legitimate interests of THIRD PARTY which are IDENTIFY Vital interests	Employment law Legal claims

Health and medical information

Purpose/Use	Lawful basis	Additional ground
• Assessment of fitness to work • Sickness absence management • In relation to reasonable adjustments • Benefit administration: to administer benefits relating to your health, medical	Contract performance Legal obligation Our legitimate interests which are IDENTIFY	Employment law Legal claims Substantial public interest

condition or disability including contractual and statutory sick pay and permanent health insurance • Health and safety: to ensure health and safety at work • Health-related departures: if you leave employment for health-related reasons, to make any applications for pensions, and permanent health insurance and DETAILS OF ANY OTHER BENENFIT purposes • Ill-health pension entitlement: to determine any entitlement to an ill-health pension under a pension arrangement operated by us • Well-being: to protect your physical, mental or emotional well-being or that of another person • Pension entitlement: to determine any entitlement under any share plan operated by us where your reason for leaving is determined to be ill health, injury or disability • Disciplinary and grievances issues • Legal disputes	Third party legitimate interests of THIRD PARTY which are IDENTIFY Vital interests	Assessment of working capacity Vital interests (incapacity)

How we use your criminal offence data

You will have been given information about whether any criminal records checks are required for your role i.e. Access NI. If checks become **OR** any further checks are required, for example, due to a change in the law or a change in your role, we will advise you.

We only use your criminal offence data when, in addition to one of the grounds that is required to process personal data (referred to previously in this notice), there is a further ground that permits us to do so. The further grounds on which we may make use of criminal offence data include:

- **Employment.** When processing criminal offence data is necessary to perform or exercise obligations or rights which are imposed or conferred by law either on us or on you in connection with employment.
- **Legal rights.** When processing criminal offence data is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings), for the purpose of obtaining legal advice, or is otherwise necessary for the purposes of establishing, exercising or defending legal rights.
- **Deemed substantial public interest.** When processing criminal offence data is deemed to be of substantial public interest because it concerns preventing or detecting unlawful acts, or protecting the public against dishonesty or because it concerns compliance with regulatory requirements in relation to unlawful acts.

Purpose/Use	Lawful basis	Additional ground
Necessary for your role Criminal offences during employment: where criminal offence data is brought to our attention during the course of your work for us (for example, if you are charged with a criminal offence) whether relating to events at or outside work Disciplinary and grievances issues Legal disputes	Contract performance Legal obligation Our legitimate interests which are IDENTIFY Third party legitimate interests of THIRD PARTY which are IDENTIFY Vital interests	Employment Legal rights Deemed substantial public interest

Data sharing

In certain circumstances, we need to share your personal data across our group of entities ie the Denomination, or with other third parties, including partners and service providers.

Any disclosures or data sharing will be done in accordance with the law or relevant contractual arrangements. All the entities in our group and other third parties are required to take appropriate security measures to protect your personal data. We only permit them to process your personal data for specified purposes and in accordance with our instructions. They are not allowed to use your personal data for their own purposes.

We will share your personal data with other group entities and service providers (including contractors and designated agents) who carry out the following functions: payroll, pension administration, benefits provision and administration, and IT services.

We will share personal data regarding your participation in any pension arrangement operated by us with the trustees or scheme managers of the arrangement in connection with the administration of the arrangements.

We may need to share your personal information with a regulator or to otherwise comply with the law. This may include making returns to HMRC, .

Cross-border data transfers

Where we transfer your personal information between **OR** from the UK and **OR** to the European Economic Area (**EEA**), those transfers are made in accordance with the UK government's adequacy decision in favour of countries in the EEA and the European Commission's adequacy decision in favour of the UK.

AND/OR

Whenever we transfer your personal information out of the UK other than between our denomination, we ensure a similar degree of protection is afforded to it by ensuring at least one of the following safeguards is implemented:

- We will only transfer your personal data to countries that have been deemed to provide an adequate level of protection for personal data
- Where we use certain service providers located outside the UK **OR** EEA, we use specific contracts approved by the UK which give personal data the same protection it has in the UK. For further details, contact our DPO.

If you would like further details on the specific mechanism we use when transferring your personal information out of the UK, contact our DPO.

Data security

We have implemented appropriate security measures to protect your personal information against accidental loss and unauthorised access, use, alteration or disclosure. Details of these measures are available from our DPO.

We impose controls for access to employee data based on business requirements and in accordance with the relevant lawful bases for processing. Any party with access rights will only process your personal information in accordance with applicable data security policies and procedures, relevant obligations or third party contractual terms.

We have put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach where we are legally required to do so.

Data retention

We will only retain your personal information in accordance with applicable laws, regulatory requirements or for as long as necessary to fulfil the purposes for which we collected it, as set out in our Data Retention Policy.

In some circumstances, you can ask us to delete your personal information. This is considered in the next section.

Once you are no longer an associated with the Denomination, we will retain and securely destroy your personal information in accordance with our Data Retention Policy and any applicable legal requirements.

Your rights in relation to your personal information

You have the following rights under data protection laws:

- **Request access** to your personal information (commonly known as making a data subject access request). We will provide you with copies of your personal information and other information, such as where we got the information from and who we have shared it with.
- **Request rectification** of the personal information that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected.
- **Request erasure** of your personal information. This enables you to ask us to delete or remove personal information where there is no good reason for us continuing to process it.
- **Request the restriction of processing** of your personal information. This enables you to ask us to suspend the processing of personal information about you, for example if you want us to establish its accuracy or the reason for processing it.
- **Request the transfer** of your personal information to another party.
- **Object to processing** of your personal information where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground. You also have the right to object where we are processing your personal information for direct marketing purposes.

If you want to exercise these rights, contact our DPO

.

No fee usually required

Ordinarily you will not have to pay a fee to exercise any of these rights. However, we may charge a reasonable fee if your request is manifestly unfounded or excessive. Alternatively, we may refuse to comply with the request.

Questions or complaints

If you have any questions or concerns about this privacy notice or how we handle your personal information, or if you wish to exercise any of the rights it refers to, contact our DPO who has been appointed to oversee compliance with this privacy notice and whose contact details are currently the Clerk of General Synod.

You have the right to make a complaint at any time to the Information Commissioner's Office (**ICO**). The ICO's contact details are available on from the ICO's website *Information Commissioner's Office*

OR as follows:

The ICO's address:

Information Commissioner's Office

Wycliffe House

Water Lane

Wilmslow

Cheshire

SK9 5AF

Helpline number: 0303 123 1113