CODE OF CONDUCT FOR CONVENERS AND MEMBERS OF BOARDS AND COMMITTEES OF THE GENERAL SYNOD

1. Introduction

Individuals serving on Boards of Committees of the General Synod are appointed in a variety of ways. Some are appointed by their diocese to serve as a diocesan representative, others are elected by General Synod, others are appointed by Boards. Whilst, for the purposes of charities legislation, the members of the Standing Committee are regarded as the charity trustees of the General Synod, it is appropriate that all members of Boards or Committees adhere to the same general principles as are applicable specifically to charity trustees. This Code of Conduct is intended to provide guidance for those serving on Boards and Committees. References to "members" of such Boards or Committees include those who are appointed to serve as "conveners" of such bodies.

2. General Principles

Service
You have a duty to act in accordance with the interests of the Scottish Episcopal Church. This means you will be expected to devote an appropriate amount of time to the work of the Board or Committee to which you are appointed, including regular attendance at meetings.

Selflessness
You have a duty to take decisions solely in terms of the Church's interests. You must not act for personal gain or financial or other material benefit (whether for yourself, family or friends).

Integrity and honesty
You must not place yourself under any financial, or other, obligation to any individual or organisation that might reasonably be thought to influence you in the performance of your duties. You must declare any private interests relating to your Church duties and take steps to resolve any conflicts in a way that protects the Church's interests.

Accountability and Stewardship
You are accountable for your decisions and actions to the General Synod. You have a duty to consider issues on their merits, taking due account of the views of others, and must ensure that the Church uses its resources prudently and in accordance with the law.

Openness and confidentiality
You should be as open as possible about all the decisions and actions that you take. You should be prepared to give reasons for your decisions and restrict information only when the wider Church interest clearly demands this. When information has to be confidential, you are required to ensure that you respect this.

Leadership
You have a duty to promote and support these principles by leadership and example, and to maintain and strengthen trust and confidence in the integrity of the Church in the conduct of business.

3. Financial matters

Guidance on a variety of finance-related matters is provided for those serving on Boards or Committees (in the paper entitled Membership of Provincial Boards/Committees). That includes information regarding the reimbursement of expenses and also incorporates the General Synod's Anti-Bribery Policy, Fraud Policy, Fraud Response Plan and Register of Gifts and other Benefits. You are expected to familiarise yourself with those documents and act in accordance with them.

4. Confidentiality and Data Protection

In serving on a provincial Board or Committee, there will be times when you will be required to treat discussions, documents or other information in a confidential manner. You will often receive information of a private nature which is not yet public, or which perhaps would not be intended to be public. You must always respect and comply with any requirement to keep such information private; if you need further information or guidance on this, you can seek clarification from the Convener, the General Office Staff member who acts as the secretary to your Board or Committee or the Secretary General.

As a member of a Board or Committee you may become aware, or come into possession, of personal data relating to individuals. Use of any such data which comes into your knowledge or possession must be restricted to the particular purpose for which it may be supplied to you and must be kept confidential. Where such data is held on personal electronic devices or home computers, such devices should be password protected and files containing personal data should be similarly password protected and held by you for no longer than is necessary. A copy of the General Synod Data Protection Policy is appended to this document and you should comply with its terms.

5. Other Organisations

You may be appointed by your Board or Committee as a member of another body or organisation. If so, you are bound by the rules of conduct of these organisations and should also observe the rules of this Code in carrying out the duties of that body. Members who are appointed as trustees of other charities as nominees of the Church will assume the full duties and liabilities of a charity trustee for that other body. It is possible that a decision or action of such a charity could conflict with Church policy and that perceived or actual conflicts of interest could therefore arise for Church-nominated trustees. You are strongly advised in any such cases to seek guidance on your responsibilities. The Secretary General may be able to assist but in some cases it may be necessary to take independent legal advice. In some cases, if a conflict of interest is irreconcilable, you may have to resign from one of the bodies.

You should also remember that where you are appointed as a member of another body or organisation, you are generally appointed as a representative of the Scottish Episcopal Church and, therefore, you should be aware that in expressing views or opinions you should endeavour to represent the views of the Church rather than simply your own personal views, or at least make clear where views you express are personal ones. This is, of course, subject to what is said above about any overriding duties owed as a charity trustee or in a similar capacity to the organisation in question.

6. Declaration of Interests

You must declare any personal interest you or close members of your family may have in a matter under discussion at a meeting, particularly where a conflict of interest could arise or might be seen to arise. This could be a financial interest, for example if you work for a company to which the possible awarding of a contract is being discussed. Similarly, conflict may arise in the awarding of a grant to another organisation with which you have some connection. Conveners should also be aware of their need to maintain impartiality when, for example, their Committee is considering a grant to the diocese or congregation to which the convener belongs. There may be other occasions where the interest is non-financial, for example where the matter for decision involves the employment of a friend. Other interests could relate to:

- employment or self-employment, whether remunerated or not
- holding of a relevant office
- holding a directorship, partnership or trusteeship of another body
- membership of a professional body
- ownership of or an interest in property or land under discussion
- ownership of shares or other assets in a company under discussion

If in doubt, you may find it helpful to ask yourself whether a member of the Church acting reasonably might consider any of the above interests could potentially affect your responsibilities to the General Synod, or could influence your actions, comments or decision-making. If in doubt, you must consult the Convener of your Board or Committee or the Secretary General.

Interests should be declared at the start of a meeting if you know in advance that an appropriate item is scheduled to arise. You should, however, declare an interest at any point in the meeting if it appears appropriate. In general, you may take part in a discussion even if you have declared an interest in an item but you must not unduly influence the discussion and you must not take part in any vote on the item. If your interest in an item is significant and material to the item under consideration, you must not take any part in the discussion, or vote, and you may, at the Convener's discretion, be asked to leave the meeting for that item.

7. Governance and Management

7.1 The principal function of provincial Boards and Committees is to provide appropriate governance in relation to their respective areas of responsibility and activity. Staff employed at the General Synod Office act as the secretariat to the Boards and Committees. They are not employed directly by the Boards and Committees they serve and the management of General Synod Office staff is

a function of the Secretary General. Whilst Boards and Committees are responsible for establishing matters of general policy, it is not their role to act in a line management capacity. Members of staff themselves are required to act in a manner which is impartial and they ought not, therefore, to be asked to act in a way which unjustifiably favours or discriminates against particular individuals or interests. If matters arise which relate to the management of staff, these should be raised with the Secretary General.

7.2 At all times, members of Boards and Committees should conduct themselves in an appropriate manner. The General Synod Office has its own policy on bullying and harassment at work in relation to the conduct of staff. Conduct which constitutes bullying or harassment is unacceptable and will be treated seriously. Bullying may include offensive, intimidating, malicious or insulting behaviour, including the abuse or misuse of power intended to undermine, humiliate, denigrate or injure the recipient. Harassment is generally understood as unwanted conduct affecting the dignity of men and women which creates an intimidating, hostile, degrading, humiliating or offensive environment. It may be related to gender, sexual orientation, race, nationality, disability, religion, belief, age or any personal characteristic of the individual. The behaviour may be persistent, or an isolated incident. Conduct which amounts to bullying or harassment will be regarded as a breach of this Code of Conduct.

8. Breaches of this Code of Conduct

8.1 If it appears to the Convener of the Standing Committee that a member of a Board or Committee has breached a provision of this Code or if he or she receives a complaint from another member or interested party alleging such a breach, he or she shall arrange for a sub group ("the Sub-Group") comprising at least three members of the General Synod to deal with the complaint. Unless the Sub-Group decides that the complaint is vexatious, frivolous or without merit, namely that even if the complaint were proved it would not constitute a breach of the Code, the Sub-Group will arrange for the matter to be investigated. The member who is the subject of such an investigation will be informed of the complaint and will be interviewed to ascertain the facts. The member is required to give the investigators his/her fullest cooperation. The complaint and investigation will be handled in confidence as far as is practicable. Unless there are exceptional circumstances, the investigation will normally be completed within 56 days.

8.2 In the event that the Sub-Group considers that there has been a breach of the Code justifying action being taken, it will refer the matter to a panel comprising three members of the Standing Committee ("the Panel") to determine how the matter should be disposed of. In the deliberations of the Panel, the members of the Sub-Group may attend and make representations and the member shall also be entitled to attend and make representations in relation to the question of whether a breach has occurred and if it has, the appropriate action to be taken. Such action may include:

- censure

- removal of the member from the Board or Committee in question either temporarily or permanently
- suspension from membership of the Board or Committee in question.

8.3 Any member who is subject to such action will have the right of appeal to the Standing Committee against any penalty applied. The Standing Committee will determine how to handle any such appeal but any member of the Standing Committee who has served on the Panel will take no part in determining the appeal.

8.4 If the member whose conduct is the subject of a complaint under this Code is the convener or member of the Standing Committee, he or she will immediately withdraw from active membership of that Committee until the matter is resolved and the Standing Committee will make arrangements for another member to assume responsibility for the complaint. Similarly if the member whose conduct is the subject of a complaint under this Code is a member of a Board or Committee of the General Synod other than the Standing Committee, he or she shall immediately withdraw from active membership of the body in question pending resolution of the matter.

Adopted by Standing Committee, June 2015
Revised June 2018

Acknowledgement: parts of the above document are drawn from a similar Code of Conduct in use within the Church of Scotland to whom thanks are expressed.

Appendix

Data Protection Policy

1. Introduction

This Data Protection Policy sets out how the General Synod of the Scottish Episcopal Church ("we", "our", "us" or the “Church”) handles the Personal Data of our members, adherents, communicants, clergy, office bearers, provincial board and committee members, General Synod members, Personnel, Pension Fund members and trustees, job applicants, suppliers, website users and other third parties in compliance with the General Data Protection Regulation. Full definitions of terms used in this policy are set out in the Glossary at paragraph 14.

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 members, adherents, communicants, clergy, office bearers, provincial board and committee members, General Synod members, Personnel, Pension Fund members and trustees, job applicants, or supplier contacts, website users or any other Data Subject.

This Data Protection Policy applies to all 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. This Data Protection Policy sets out what we expect from you in order for us to comply with applicable law. Your compliance with this Data Protection Policy is mandatory. Any breach of this Data Protection Policy may result in disciplinary action.

This Data Protection Policy is an internal document and cannot be shared with third parties, clients or regulators without prior authorisation from the Secretary General.

We reserve the right to change this Data Protection Policy at any time without notice to you so please check back regularly to obtain the latest copy of this Data Protection Policy. We last revised this Data Protection Policy on 1 May 2018.

2. Scope

We recognise that the correct and lawful treatment of Personal Data will maintain confidence in the Church and will provide for successful operations. Protecting the confidentiality and integrity of Personal Data is a critical responsibility that we take seriously at all times. We are exposed to potential fines of up to EUR20 million (approximately £18 million) depending on the breach for failure to comply with the provisions of the GDPR.

All departments and staff, have a role to play in ensuring all Personnel comply with this Data Protection Policy and therefore need to implement appropriate practices, processes, controls and training to ensure such compliance.

The Secretary General is responsible for overseeing this Data Protection Policy and, as applicable, developing Related Policies and Privacy Guidelines. That post is held by John Stuart, who can be contacted on 0131-225-6357 or at secgen@scotland.anglican.org.

Please contact the Secretary General with any questions about the operation of this Data Protection Policy or the GDPR or if you have any concerns that this Data Protection Policy is

not being or has not been followed. In particular, you must always contact the Secretary General in the following circumstances:

(a) if you are unsure of the lawful basis which you are relying on to process Personal Data (including the legitimate interests that we are relying on) (see 4.1);

(b) if you need to rely on Consent and/or need to capture Explicit Consent (see 4.2);

(c) if you need to amend the Privacy Notice to reflect new processing activities or check that this have been issued (see 4.3);

(d) if you are unsure about the retention period for the Personal Data being Processed (see 8);

(e) if you are unsure about what security or other measures you need to implement to protect Personal Data (see 9);

(f) if there has been a Personal Data Breach (see 9.2);

(g) if you are unsure on what basis to transfer Personal Data outside the EU (see 11);

(h) if you need any assistance dealing with any rights invoked by a Data Subject (see 12);

(i) whenever you are engaging in a significant new, or change in, Processing activity which is likely to require a DPIA (see 13.3) or plan to use Personal Data for purposes others than what it was collected for;

(j) if you need help complying with applicable law when carrying out direct marketing activities (see 13.4); or

(k) if you need help with any contracts or other areas in relation to sharing Personal Data with third parties (see 10).

3. Personal data protection principles

We adhere to the principles relating to Processing of Personal Data set out in the 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 being in place (Transfer Limitation).

(h) Made available to Data Subjects and Data Subjects allowed to exercise certain rights in relation to their Personal Data (Data Subject's Rights and Requests).

4. Lawfulness, fairness, transparency

4.1 Lawfulness and fairness

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

You may only collect, Process and share Personal Data fairly and lawfully and for specified purposes. The 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.

The GDPR allows Processing on the basis of specific legal grounds, some of which are set out below:

(a) the Data Subject has given his or her Consent to the Processing;

(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; or

(e) to pursue our legitimate interests 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.

When Sensitive Personal Data is being processed, the GDPR mandates that additional conditions must be met. These include, among other bases:

(a) the Data Subject has given his or her explicit Consent to the Processing;

(b) the Processing is necessary for the purposes of carrying out the obligations or exercising specific rights in relation to employment so far as required by UK law;

(c) to protect the Data Subject's vital interests where the individual is physically or legally incapable of giving consent;

(d) the Processing is necessary for reasons of substantial public interest; or

(e) the Processing is necessary for the establishment, exercise or defence of legal claims.

We must only collect and use Personal Data on the basis of one or more of these lawful bases set out in the GDPR.

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

4.2 Consent

Whilst consent is a lawful basis for Processing Personal Data, we will only rely on consent as a legal basis where no other legal basis can be relied upon for the Processing of Personal Data, such as for the collection of Sensitive Personal Data or where we wish to communicate with members for promotional purposes by electronic communications such as e-mail and text message. You should always try to identify if there is another legal basis for Processing of Personal Data on which we could rely.

A Data Subject consents to Processing of their Personal Data if he or she indicates agreement clearly either by a statement or positive action to the Processing. Consent requires affirmative

action so silence, pre-ticked boxes or inactivity are unlikely to be sufficient. If Consent is given in a document which deals with other matters, then the Consent must be kept separate from those other matters.

Data Subjects 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.

You will need to evidence Consent captured and keep records of all Consents so that we can demonstrate compliance with Consent requirements.

4.3 Transparency (notifying data subjects)

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

Whenever we collect Personal Data directly from Data Subjects we must provide the Data Subject with all the information required by the GDPR including the identity of the Data Controller and explaining why we are collecting the Personal Data, what we will do with the Personal Data, how long the Personal Data will be held for, to whom we may disclose the Personal Data and who Data Subjects should contact if they have any questions about how their Personal Data is used.

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

If you want to use Personal Data for additional/new purposes that are not provided for in the existing version of the Privacy Notice, then the Privacy Notice must be updated to provide for this new use and Data Subjects must be informed of this new use of their Personal Data

5. Purpose limitation

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.

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.

6. Data minimisation

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

You may only Process Personal Data when performing your role requires you to do so. You must not Process Personal Data for any reason unrelated to your role.

You may only collect Personal Data for specified, explicit and legitimate purposes and where there is a valid business reason for doing so: do not collect excessive data. Ensure any Personal Data collected is adequate and relevant for the intended purposes.

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

7. Accuracy

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

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.

8. Storage limitation

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.

We will maintain retention policies and procedures to ensure Personal Data is deleted after a reasonable time for the purposes for which it was being held, unless a law requires such data to be kept for a minimum time. You must comply with our guidelines on data retention.

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 our applicable guidelines on data retention. This includes requiring third parties to delete such data where applicable.

9. Security integrity and confidentiality

9.1 Protecting Personal Data

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

We will develop, implement and maintain safeguards appropriate to our size, scope and operations, 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 Sensitive Personal Data from loss and unauthorised access, use or disclosure.

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 in compliance with section 10 and 11 below.

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

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

(b) Integrity means that Personal Data is accurate and suitable for the purpose for which it is processed.

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

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

9.2 Reporting a Personal Data Breach

The GDPR requires Data Controllers to notify any Personal Data Breach to the applicable regulator within 72 hours of becoming aware of the Personal Data Breach. In certain instances, we may also be required to notify Data Subjects affected by Personal Data Breaches that are likely to result in a high risk to the Data Subject without undue delay.

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

If you know or suspect that a Personal Data Breach has occurred, **do not attempt to investigate the matter yourself**. Immediately contact the Secretary General and follow the Data Security Breach Policy. You should preserve all evidence relating to the potential Personal Data Breach.

A Personal Data Breach covers a wide range of scenarios and could cover, but is not limited to:

(a) sending Personal Data relating to one member to another member;

(b) Personal Data being lost in the post (for example it is sent but does not arrive with the intended recipient);

(c) a laptop being misplaced – even if the laptop is encrypted and subsequently recovered;

(d) the loss of a CD/USB with unencrypted data on it;

(e) sending an email with an incorrect link or attachment containing any Personal Data such that Personal Data is shared with an unintended recipient; or

(f) a malware attack which accesses Personal Data.

10. Sharing Personal Data

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

You may only share the Personal Data we hold with another entity if the recipient has a job-related need to know the information and the transfer complies with any applicable cross-border transfer restrictions.

You may only share the Personal Data we hold with third parties, such as our Vestries or 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 GDPR approved third party clauses has been obtained.

You must also comply with any guidelines issued by us on sharing data with third parties. Examples of sharing personal data include the issuing of the Red Book and the Blue Book.

11. Transfer limitation (transfers outsider the EU)

The GDPR restricts data transfers to countries outside the EU in order to ensure that the level of data protection afforded to individuals by the 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.

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

(a) the European Commission has issued a decision confirming that the country to which we transfer the Personal Data ensures an adequate level of protection for Data Subjects' rights and freedoms;

(b) appropriate safeguards are in place such as binding corporate rules (BCR), standard contractual clauses approved by the European Commission, an approved code of conduct or a certification mechanism;

(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 GDPR including the performance of a contract between us and the Data Subject, reasons of public interest, to establish, exercise or defend legal claims or to protect the vital interests of the Data Subject where the Data Subject is physically or legally incapable of giving Consent.

You must comply with any guidelines we issue on cross border data transfers. If you have any questions about the above conditions, please speak to the Secretary General.

12. Data Subject's rights and requests

Data Subjects have 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 Data Controller's Processing activities (“right to be informed”);

(c) request access to their Personal Data that we hold (“right of access”);

(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 (“right to be forgotten”);

(f) restrict Processing in specific circumstances (“right to the restriction of processing”);

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

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

(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 the supervisory authority; and

(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 (“right to data portability”).

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).

You must immediately forward any Data Subject request you receive to Secretary General and comply with any Data Subject response process or specific instructions we give you.

13. Accountability

13.1 Record keeping

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

You must keep and maintain accurate records reflecting our Processing including records of Data Subjects' Consents and procedures for obtaining Consents in accordance with our record keeping guidelines.

These records should include, at a minimum, the name and contact details of the Data Controller, clear descriptions of the Personal Data types, Data Subject types, Processing activities, Processing purposes, third-party recipients of the Personal Data, Personal Data storage locations, Personal Data transfers, the Personal Data's retention period and a description of the security measures in place.

We must create and maintain a Data Processing Register and provide it to the relevant regulators on request to demonstrate our compliance with GDPR.

The Data Processing Register must include as a minimum what Personal Data is held, where it is held, why, where it is sent, how long it is to be held and the Processing which is done on it – this should be done by reference generally to the relevant categories of Personal Data.

The Data Processing Register must be monitored, aligned to our retention policy and be kept up to date.

13.2 Training and audit

We are required to ensure all 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.

You must undertake all mandatory data privacy related training and ensure your team undertakes similar mandatory training.

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.

13.3 Privacy By Design and Data Protection Impact Assessment (DPIA)

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. Privacy by Design means that the protection of Personal Data must be considered in the early stages of any project and throughout its lifecycle as well as when carrying out day-to-day activities. The protection and effective use of Personal Data must be at the forefront of minds and must not be an afterthought.

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

(a) current industry standards;

(b) the cost of implementation;

(c) the nature, scope, context and purposes of Processing; and

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

Under the GDPR, if and when you process data in a way that is likely to present a high data privacy risk, you must now conduct a data protection impact assessment (DPIA).

A DPIA is used to identify, evaluate and mitigate the potential risks and impacts that processing activities might have on data subjects. Generally, a DPIA is conducted at the start of a project that could have data protection or privacy implications, e.g. rolling out a new HR system.

DPIAs are a preventative measure—if data security risks are assessed and addressed at the start of the project, you are less likely to need remedial action part way through the project or suffer a breach.

A DPIA must include:

(a) a description of the Processing, its purposes and the Data 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; and

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

You must comply with our guidelines on DPIA and Privacy by Design.

13.4 Direct marketing

We are subject to certain rules and privacy laws when marketing to our members.

For example, a Data Subject's prior consent is required for electronic direct marketing (for example, by email, text or automated calls).

The right to object to direct marketing must be explicitly offered to the Data Subject in an intelligible manner so that it is clearly distinguishable from other information.

A Data Subject's objection to direct marketing must be promptly honoured. If an individual opts out at any time, their details should be suppressed as soon as possible. Suppression involves retaining just enough information to ensure that marketing preferences are respected in the future.

You must comply with any guidelines on direct marketing to individuals.

14. Glossary

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 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.

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, signifies agreement to the Processing of Personal Data relating to them.

Data 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 GDPR. We are the Data Controller of all Personal Data relating to our Personnel and Personal Data used in our business for our own commercial purposes.

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. DPIA can be carried out as part of Privacy by Design and should be conducted for all major system or business change programs involving the Processing of Personal Data.

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

General Data Protection Regulation (GDPR): means all applicable legislation and regulations relating to the processing of personal data and privacy including (without limitation) the Data Protection Act 1998 and any regulations or instruments enacted under that Act, the European Union General Data Protection Regulation 2016/679 as, when and where it comes into and remains in force and/or any corresponding or equivalent national laws or regulations, the Privacy and Electronic Communications (EC Directive) Regulations 2003 and the Data Protection (Processing of Sensitive Personal Data) Order 2000 or any amendments and/or re-enactments of any of them.

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 Sensitive 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 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.

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

Privacy by Design: implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the GDPR.

Privacy Notices: notices setting out information that may be provided to Data Subjects when we collect information about them.

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.

Sensitive 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, and Personal Data relating to criminal offences and convictions.