DATA PROTECTION POLICY

Contact Details: Unit 24, SHBP, Majors Road, Watchfield, SN6 8TZ; 01793 783123

The prudent keep their knowledge to themselves, but a fool's heart blurts out folly. (NIV – Prov 12:23)

1. ICO Reference

Reference Number - Z5395056. Date of Renewal **3 Mar 21.**

All organisations which process personal data must be registered with the Information Commissioner's Office (ICO). Currently, the DCN is registered with the ICO for the following purposes:

- Pastoral Support
- Accounts and Records
- Advertising, Marketing and Public Relations
- Staff Administration
- Administration of Membership Records
- Fundraising
- Realising the Objectives of a Charitable Organisation or Voluntary Body

2. Introduction, Scope and Context

2.1 Introduction

This document sets out the policy, practice and responsibilities adopted by the Defence Christian Network (DCN) to meet its legal obligations under the Data Protection Act 1998, as amended by the EU Regulation 2016/679 General Data Protection Regulation (GDPR) and which will be embedded into national law post Brexit with effect from 1 January 2021 as part of "EU retained law".

It should be read in conjunction with other DCN GDPR compliance documents, such as the staff and website privacy statements which set out how data relating to individuals is used by the DCN in the course of its charitable business.

2.2 Scope

This policy describes how personal data must be collected, handled, processed, transferred and stored to meet the standards set by the Board of Trustees and to comply with the law.

It applies to all DCN staff, trustees, associated organisations, suppliers and other people the Union has a relationship with or may need to contact. For ease, the term 'staff' is used throughout this policy to refer to employees, officers, consultants, (sub-)contractors, volunteers, interns, casual workers and agency workers.

This policy does not form part of any employee's contract of employment and may be amended at any time.

It applies to all data held by the DCN relating to identifiable individuals, even if that information technically falls outside of the Data Protection Act 2018.

This can include:

- Names of individuals
- Rank and service number of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- Gender
- Marital status
- Names and ages of children (where appropriate)
- Other personal relevant information

2.3 Context

The Data Protection Act 2018 describes how organisations including DCN must collect, handle and store personal information. These rules apply regardless of whether data is stored electronically, on paper or other materials. To comply with the law, personal information must be collected, used fairly, stored safely and not disclosed unlawfully. We recognise too that the correct and lawful treatment of personal data maintains confidence in the Charity.

3. Definition of Data Protection Terms

3.1 Data

This is information which is stored electronically, including on a computer or 'in the cloud', or in certain paper-based filing systems.

3.2 Data subjects

For the purpose of this policy these include all living individuals about whom we hold personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal information

3.3 Personal data

This means data relating to a living (“natural”) individual (“data subject”) who can be identified from that data (or from that data and other information in our possession) whether directly or indirectly. Personal data can be factual (e.g., a name, address, date of birth, identify number or online identifier); it can refer to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person; or it can be an opinion about that person, their actions and behaviour.

3.4 Data controllers

These are the people who or entities which determine the purposes and the manner in which any personal data is processed. They are responsible for establishing practices and policies in line with the Act. We are the data controller of all personal data used in the running of DCN.

3.5 Data users

These are those of our staff, including trustees and associated organisations whose work and service involve processing personal data. Data users must protect the data they handle in accordance with this data protection policy and any applicable data/ IT security procedures at all times.

3.6 Data processors

These include any person or entity that is not a data user who/ that processes personal data on our behalf and on our instructions. Staff of data controllers are excluded from this definition, but it could include third parties which handle personal data on DCN's behalf.

3.7 Processing

This is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including collecting, structuring, organising, amending, retrieving, using, disclosing, disseminating, erasing or destroying it. Processing also includes transferring personal data to third parties.

3.8 Sensitive personal data

This includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexual life, or about the commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings. Sensitive personal data can only be processed under strict conditions, including a condition requiring the express permission of the person concerned. In order to process these types of data consent from the data subject must be obtained by the organisation handling the data. Explicit consent must be given when it is sensitive personal data.

The term 'personal data' used throughout this policy should be taken to include both kind of 'personal' and 'sensitive personal' data.

4. Responsibilities

4.1 Who is responsible?

The DCN will do its utmost to ensure that all its staff, trustees, members and third party suppliers are conversant with data protection legislation and practice.

Everyone who works for or with DCN, whether on a paid or voluntary basis, has some responsibility for ensuring data is collected, stored and handled appropriately. However, certain people have key areas of responsibility.

4.2 Board of Trustees

The Board of Trustees is ultimately responsible for ensuring the DCN meets its legal obligations.

4.3 Operations Director

The Operations Director is responsible for the overall implementation of this policy as the Data Protection Officer, in particular:

- Keeping the Board updated about data protection responsibilities, risks and reviews,

contributing to periodic reports, meetings, etc as needed

- Reviewing all data protection procedures and related policies in line with the agreed schedule and keeping them up-to-date, including to reflect any new legal developments
- Arranging data protection training and advice for people covered by this policy
- Handling data protection questions from staff and anyone else covered by this policy
- Ensuring that DCN's database and all other processes (whether in electronic or other form) are maintained in a data protection compliant manner
- Ensuring that adequate insurance is in place should any data breaches occur, and that all requirements for insurance cover to be valid (e.g., the existence of certain policies or procedures required for any cyber and data breach insurance) are met
- Ensuring that DCN's registration with the Information Commissioner's Office is kept up-to-date and renewed annually
- Ensuring that all data protection registers, records, forms, etc required by law or representing good practice are maintained and kept up-to-date
- Dealing with requests from individuals in relation to the data DCN holds about them (e.g., "subject access requests", requests for erasure or correction – see further sections 11 and 12 below)
- Checking and approving any contracts or agreements with third parties that may handle the Union's data or have access to the Union's IT (e.g. Complete IT, ChurchSuite)
- Approving any data protection statements attached to communications such as emails or letters
- Addressing any data protection queries from outside agencies (including journalists, media outlets or the ICO)
- Ensuring all marketing and promotional initiatives abide by data protection principles

4.4 IT Provider

Complete IT is responsible for:

- Ensuring all systems, services and equipment used for storing data meet acceptable security standards
- Performing regular checks and scans to ensure security hardware and software is functioning properly
- Approving and recommending software to prevent malicious threat and data theft

4.5 Administrative Coordinator

The Administrative Coordinator is responsible for ensuring the information collected and stored by the DCN (e.g. on ChurchSuite) does not breach the data protection policy.

5. Use of Personal Information

5.1 Personal information held

The DCN holds personal information about living individuals, especially staff, trustees, supporters and other individuals who have provided such information for specific purposes relating to the work of the Union.

During the course of our activities we collect, store and process personal data about past, current and prospective members, supporters, staff and other third parties with whom we communicate.

5.2 Use of personal information

The principal purposes for which this personal information is used include:

- For the purpose of maintaining the DCN database
- The day-to-day administration of DCN, such as managing Human Resources matters, maintaining training records, and maintaining financial records of giving for audit, tax and Gift Aid purposes
- The administration of DCN organised events and activities
- Communication with members and supporters whose contact details we hold to keep them informed of relevant DCN activities and events
- To organise and coordinate prayer activities, including regional prayer groups and coordination with serving members linked up to them
- Maintaining confidential records of DCN staff and trustees (e.g., employee/ contractor contracts, volunteer agreements, confidential appraisals)
- For the purpose of disciplinary, grievance or employee performance improvement issues
- For organising, coordinating and giving pastoral support, prayer ministry and discipleship to members
- For the purposes of legal proceedings
- For compliance with legislation

All personal information which is held by the DCN will be treated as private and confidential and only disclosed to those persons involved in the administration and day-to-day ministry of the DCN, unless otherwise agreed with the data subject.

5.3 Data protection risks

This policy is important not only because it helps us to meet our legal compliance obligations, but also due to the real risks associated with the handling and use of data. These can take many forms, for instance:

- Breaches of confidentiality which can undermine trust and hinder the fulfilment of our charitable mission
- Reputational damage which can impact negatively upon our support base
- Inappropriate use of personal data which does not offer genuine choice to individuals concerning how their data is used, thereby undermining trust
- Insufficient security measures which lead to a data breach which could cost the Union significant

sums of money in terms of ICO fines, personal data monitoring, etc

6. Data Protection Principles

The DCN fully endorses and adheres to the principles of good practice of the GDPR detailed below. These principles specify the legal conditions that must be satisfied in relation to obtaining, handling, processing, transportation and storage of personal data. All persons and other entities covered by the scope of this policy, who obtain, handle, process, transport and store personal data for the DCN, must adhere to these principles.

Seven principles lie at the heart of the general data protection regime. These are that all personal data must be:

- Processed fairly, lawfully and in a transparent manner
- **Collected for specified, explicit and legitimate purposes** and not further processed in a manner that is incompatible with those purposes
- **Adequate, relevant and limited** to what is necessary in relation to the purposes for which they are processed. This does not mean that the processing of data has to be essential; rather that it must be a targeted and proportionate way of achieving the stated purpose of the processing of any data
- **Accurate and, where necessary, kept up to da**te. Every reasonable step must be taken to ensure that personal data are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay
- Kept in a form which permits identification of data subjects for **no longer than is necessary** for the purposes for which the personal data are processed. This will depend on various factors, such as legal limitation or specified periods we are required or advised to retain records for
- **Processed in a manner that ensures appropriate security** of the personal data to protect its integrity and confidentiality, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures
- **Accountability**, namely that any data controllers or processors take responsibility for complying with these principles, and have appropriate processes and records in place to demonstrate that compliance

7. Lawful, Fair and Transparent Data Processing

Data protection legislation is not intended to prevent the processing of personal data, but rather to ensure that it is done lawfully, fairly and transparently, without adversely affecting the rights of the data subject. Its provisions are more extensive than those of the Data Protection Act 1998, with the GDPR placing more emphasis on accountability for and transparency about the lawful basis relied upon for data processing.

For personal data to be processed lawfully, they must be processed on the basis of one or more of the legal grounds set out in the GDPR. These specified legal bases are as follows:

- **Consent:** DCN has been given clear consent for us to process personal data for a specific purpose.
- **Contract**: the processing is necessary for a contract we have with the data subject or because they have asked us to take specific steps before entering into a contract.
- **Legal obligation:** the processing is necessary for us to comply with the law (not including contractual obligations).
- **Vital interests:** the processing is necessary to protect someone's life.
- **Public task:** the processing is necessary for us to perform a task in the public interest or for our official functions, and the task or function has a clear basis in law.
- **Legitimate interests:** the processing is necessary (i.e. conducted in a targeted and proportionate way) for our legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the data subject's personal data which overrides those legitimate interests (i.e. a balancing test has been undertaken between our legitimate interests and your interests, rights and freedoms to assess whether your interests override our legitimate interests). When this legal basis is relied upon, we are under an obligation to keep it under review.

8. Criminal Offence Data Processing

Criminal offence data is personal data relating to criminal convictions and offences, or related security measures.

In order to lawfully process special category data, we are required to identify both a lawful basis to process the data as well as identify a separate condition for processing special category data. For example, this could take the form of obtaining consent from the members we support whilst serving custodial sentences in prison.

9. Keeping Data Subjects Informed

The DCN shall provide the following information to all of its data subjects:

- Where personal data is collected directly from staff and trustee data subjects, those data subjects will be informed of its purpose at the time of collection, and
- Where personal data is obtained from a third party, the relevant data subjects will be informed of its purpose when the first communication is made with them, before any transfer is made, or as soon as reasonably possible (and not more than one month after the personal data is obtained).

Furthermore, all data subjects will be provided with the following details: the legal basis (legitimate interest relied upon); the category of personal data collected and processed; any third parties to whom data is transferred; data retention; and the data subject's rights under GDPR (e.g., to withdraw their consent, or to complain).

The DCN aims to ensure that individuals know what data is being held, and they understand:

- How the data is being used

- How to exercise their rights
- How to restrict the amount and type of data that is shared with other members

10. Processing in Line with Data Subject's Rights

We will process all personal data in line with data subjects' rights, in particular their:

- Right to be informed about the collection and use of their personal data
- Right of access to any data held about them by a data controller (see also clause 11)
- Right to rectification (see also clause 12)
- Right to erasure (see also clause 12)
- Right to restrict processing (see also clause 12)
- Right to data portability (see also clause 12)
- Right to object (see also clause 12)

11. Dealing with Subject Access Requests

11.1 What is a Subject Access Request (SAR)?

All DCN data subjects may make a Subject Access Request (SAR) at any time to find out more about the personal data which the Charity holds about them, what it is doing with that personal data, and why.

Data subjects may make a SAR either verbally or in writing. This request must relate to their personal data only; the personal information relating to other people cannot normally be requested. Any DCN staff and trustees receiving a written request should forward it to their manager immediately.

11.2 What Data may be Requested?

Data subjects have the right to obtain the following information from us:

Confirmation that we are processing their personal data

A copy of their personal data

Other supplementary information

11.3 Conditions to be met for a SAR

In making a SAR orally, the following conditions need to be met:

- We will check the caller's identity to make sure that information is only given to a person who is entitled to it. Such identity confirmation should involve verifying at least three items of personal data, such as date of birth, home address, personal phone number
- We will require that the caller puts their request in writing if we are not sure about the caller's identity and where their identity cannot be checked

A standard SAR form is at Appendix 1 to this policy. It is not, however, essential for this form to be used. SARs may be made by any means, e.g. in the form of a letter, email or verbally.

11.4 Legalities

Under GDPR, we have **one month** in which to respond to such a request, acting without undue delay. If the request is complex or if multiple requests from the same person have been received, we may extend the time to respond by a further two months.

Normally, no fee will be charged to comply with the SAR, unless it is considered to be manifestly unfounded or excessive, or further copies of data are requested following a request. In such circumstances, a 'reasonable fee' may be charged for the administrative costs associated with complying with the request.

In certain circumstances, we can refuse to respond to a request (e.g., if it would disclose information about another individual who can be identified from the information unless, for instance, that person has consented to such disclosure; or if the request is manifestly unfounded or excessive); or we can extend the time limit to respond to a request (e.g., due to its complexity).

12. Dealing with other Requests

Under the GDPR, there are a number of other requests which data subjects may make which are outlined briefly here.

12.1 Request for rectification.

This is the right to have inaccurate personal data rectified or completed if it is incomplete. Personal data is inaccurate if it is incorrect or misleading as to any matter of fact.

12.2 Request for erasure.

This is the right for data subjects to have personal data erased, otherwise known as “the right to be forgotten”. This applies in certain circumstances, such as if:

- The personal data is no longer necessary for the purpose for which the DCN originally collected or processed it
- If consent, forming the legal basis for holding data, is withdrawn by the data subject
- The data subject objects to the holding and processing of their personal data (and there is no overriding legitimate interest to allow the DCN to continue doing so)
- The personal data has been processed unlawfully, or
- The personal data needs to be erased (or in some instances not erased) in order for the DCN to comply with a particular legal obligation

In certain circumstances, the right to erasure will not apply if processing is necessary:

- To exercise the right of freedom of expression and information
- To comply with a legal obligation
- For the establishment, exercise or defence of legal claims

12.3 Request to restrict processing.

This is the right of a data subject to request the restriction or suppression of their personal data in certain circumstances as an alternative to requesting the erasure of their data.

This right may be exercised in certain circumstances, including:

- If the data subject contests the accuracy of their personal data and the DCN is verifying the accuracy of the data
- The data has been unlawfully processed (i.e. in breach of the lawfulness requirement of the first principle of the GDPR)
- The DCN no longer needs the personal data but the data subject needs to keep it in order to establish, exercise or defend a legal claim

The restriction of data may take a number of different forms, for instance:

- Temporarily moving the data to another processing system
- Making the data unavailable to users, or
- Temporarily removing published data from a website

12.4 Request to data portability.

The right to portability allows data subjects to obtain and reuse their personal data for their own purposes across different services. For instance, it allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without affecting its usability.

12.4.1 Structure

The data should be supplied in a manner that is structured (i.e. allows for easier transfer and increased usability), commonly used (i.e. widely used and well-established) and in machine-readable (i.e. can be automatically read and processed by a computer) format. This right only applies to information an individual has provided to a data controller.

12.4.2 Right to Portability

The right to data portability only applies when the legal basis for holding personal data is consent or the performance of a contract, or the DCN is carrying out data processing by automated means.

12.5 Dealing with an objection.

The GDPR gives individuals the right to object to the processing of their personal data in certain circumstances. They have an absolute right to object if the processing of their data is for direct marketing purposes.

The timelines, format, restrictions, and (non) payment of fees are very similar to those for Subject Access Requests.

13. Data Security

The DCN takes appropriate security measures against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.

We will put in place appropriate technological and organisational measures (such as organisational policies, physical or technical measures) to maintain the security of all personal data from the point of collection to the point of destruction as is required by the GDPR.

We will maintain data security by protecting the confidentiality, integrity and availability of the personal data. This includes through the implementation of office routines and protocols, such as file sharing (via MS 365) rather than emailing personal information, good email and electronic filing housekeeping, appropriate use of privacy markings such as “confidential”; as well as through various security measures such as passwords, encryption, regular back-ups, use of lockable storages, shredding, etc.

14. Personal Data Breaches

14.1 Duty to Report Personal Data Breaches

The GDPR requires the DCN to report certain types of personal data breach to the relevant supervisory authority **within 72 hours** of becoming aware of the breach, where feasible. Where the breach is likely to result in a **high risk** of adversely affecting individuals' rights and freedoms, we must inform data subjects of this without **undue delay**.

A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data.

It means that a breach of security has occurred leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes.

14.2 Examples of Data Breaches

Specific examples of common personal data breaches are:

- Access by an unauthorised third party
- Deliberate or accidental action (or inaction) by a controller or processor
- Sending personal data to an incorrect recipient
- Computing devices containing personal data being lost or stolen
- Alteration of personal data without permission, and
- Loss of availability of personal data

It is essential that the Data Protection Officer is notified immediately anyone (e.g., data subject or DCN staff) becomes aware of any suspected breach of personal data. If the breach is likely to pose a risk to the data subject (e.g., emotional distress, physical and/or material damage such as financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage) then the Information Commissioner’s Office must be notified.

15. Transferring Personal Data to a Country Outside of the EEA

Should personal data held by the DCN be transferred outside of the European Economic Area ("EEA") to a third country then special requirements exist which must be followed. This includes seeking the data subject’s informed consent; ensuring that the transfer is necessary for one of the reasons set out in the GDPR; to protect the vital interests of the data subject; for public interest grounds; or for the establishment, exercise or defence of legal claims.

The position regarding the UK's obligations in relation to the EEA and, whether the UK itself will be considered to fall outside of the EEA, is currently unclear until Brexit negotiations have been completed and such legalities have been determined.

16. Disclosure and Sharing of Personal Information

The DCN takes the security and confidentiality of personal data extremely seriously. In certain circumstances, the DCN may disclose personal data we hold to third parties. Unless required by law this will not include the sharing of sensitive personal data:

- If we are under a duty to disclose or share a data subject's personal data in order to comply with any legal obligation (e.g, for crime or taxation purposes)
- There is a public duty to disclose (e.g, under a UK enactment)
- Disclosure is required to protect the interests of the individual concerned
- For the purpose of seeking legal advice and related proceedings
- The individual concerned has requested (or given their consent to) the data being disclosed (e.g, for the purpose of a confidential reference, or to enable another e.g. another UK-based Christian organisation to provide them with pastoral support)
- In order to enforce or apply any contract with the data subject or other agreements
- To protect our rights, property, or safety of our employees, customers, or others. This includes exchanging information with other companies and organisations for the purposes of fraud protection and credit risk reduction

The DCN requires a Confidentiality Agreement Statement to be signed by other UK Military Christian organisations before any data is released. In addition, these organisations MUST have robust data protection policies of their own. DCN staff are required to check their personal data processing arrangements before sharing any personal details. (Template available at Appendix 2).

17. Policy Implementation

Detailed guidance regarding the practical implementation of this policy is available at Appendices 3-4.

18. Changes to this Policy

The DCN reserves the right to change this policy at any time, which it keeps under regular review and updates when necessary. Where appropriate, it will notify data subjects of those changes by mail or email.

19. Policy Review

This policy should be reviewed annually.

Last reviewed: December 2020

APPENDIX 1: SUBJECT ACCESS REQUEST FORMS

Subject Access Request Form

Under the GDPR, you have a right of access to personal information that the Defence Christian Network holds about you.

Completing this form will help us to locate the information you are seeking and deal with your request as quickly as is possible. Alternatively, the same details may be passed orally to us.

Part 1 – About Yourself

Full Name:

Current Address:

Previous Address (if relevant):

Phone Number:

Email Address:

Date of Birth:

Part 2 - Locating Your Personal Information

In order for us to be able to locate the information you are seeking, please provide some details, if known, as to where/by whom you feel information is held about you.

Data Details:

(e.g., what type of data, any dates, where and how might be held).

Name of Persons Holding Requested Details:

Any Additional Information:

(Please continue of a separate piece of paper if necessary)

APPENDIX 2: DCN Confidentiality Agreement Statement

DCN Data Protection Policy

I have read the DCN Data Protection Policy and will protect the data shared with me in accordance with DCN policy.

Disclosure to other Organisations

The DCN will not pass personal data to other third parties. This means the DCN will not sell/ exchange its data to/with other organisations.

Disclosing Data for Other Reasons

In certain circumstances the Data Protection Act allows personal data to be disclosed to law enforcement agencies without the consent of the data subject. There are also circumstances where the law allows DCN to disclose data (including sensitive data) without the data subject's consent.

These are:

- Carrying out a legal duty or as authorised by the Secretary of State
- Protecting vital interests of an Individual /Service User or other person
- The Individual/Service User has already made the information public
- Conducting any legal proceedings, obtaining legal advice, or defending any legal rights
- Monitoring for equal opportunities purposes – i.e. race, disability or religion
- Providing a confidential service where the Individual/Service User's consent cannot be obtained or where it is reasonable to proceed without consent: e.g. where we would wish to avoid forcing stressed or ill Individuals/Service Users to provide consent signatures

Correct Processing of Personal Data

The DCN regards the lawful and correct treatment of personal information as very important to our successful working, and to maintaining the confidence of those with whom we deal. Under these circumstances the DCN will disclose requested data. However, the Operations Director will ensure the request is legitimate, seeking advice from the board and legal advice where necessary.

Signed:

Name:

Dated:

APPENDIX 3: General Staff Guidelines

General Principles for Policy Implementation

The only people able to access data covered by this policy should be those who need it for their work. This includes those who work voluntarily for the Union as Local DCN Reps, Prayer Support Team Leaders and Steering Group Chairs. There are different levels of access to data depending on role meaning that data is accessed only on a need to know basis.

Data should never be shared informally and without the knowledge of the person whose data is being shared.

Staff must keep a record of all processing actions under the GDPR regulations, e.g. by recording when (and what) data is shared with another individual or MCO.

Staff should keep all data secure, by taking sensible precautions following the guidelines below:

- Strong passwords should be used on computers. These should not be shared
- Personal data should not be disclosed to unauthorised people. This includes giving a member's address/email/telephone number to another member
- Data should be regularly reviewed and updated if it is found to be out of date. If it is no longer required, it should be deleted and disposed of
- Staff should request help from their line manager or the Operations Director if they are unsure about any aspect of data protection
- When using Email distribution lists, send blind copies
- When setting up a new contract with outside organisations, staff are to ensure that their procedures are compliant with DCN policy and GDPR

A checklist to ensure compliance with these guidelines is included in Appendix 4.

Data Storage

Data Stored on Paper

When data is stored on paper it should be kept in a secure place where unauthorised people cannot see it. These guidelines also apply to data that is usually stored electronically but has been printed out for some reason.

The following guidelines should be followed by employees/ volunteers with access to data:

- When not required the paper or files should be kept in a closed opaque file or filing cabinet
- Paper and printouts should not be left where unauthorised people could see them
- Papers containing data should be shredded and disposed of securely when no longer required

Data Stored Electronically

When data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts.

- It should be protected by strong passwords
- If it is stored on removeable media (like DVD, USB), these should be kept securely and put away in a secure location when not in use
- Data should be only stored on designated drivers and servers and should only be uploaded to an approved cloud computing service such as ChurchSuite, and MS Teams. These must be located in the EEA
- Data should be backed up regularly
- All servers and computers containing data should be protected by an approved security software and a firewall
- Personal data should never be transferred outside of the EEA
- Data should be held in as few places as necessary
- Staff should take every opportunity to ensure data is updated. For instance, by confirming a member's details when they call
- DCN will make it easy for data subjects to update the information the DCN holds about them. Individuals have access to their own data through a password using the ChurchSuite App, and are able to update their details and decide how visible their data is to other members

Adding Individuals to the Database

When individuals are being added to the DCN's database they need to be informed of how their information will be stored and used. This means that the DCN Data Privacy Statement needs to be referenced in all our written requests for data. A verbal statement should be used for phone, email or face-to-face collection. (These statements are not required if the way the data is collected makes it obvious how it will be used).

The DCN data protection statement must appear on all forms that people complete as a means of registering with the DCN, including those on the web. If they have not completed a form which includes the data protection statement, then the statement must be included in a letter or email to the individual.

Permission must be sought and recorded to use/store sensitive data.

Personal Data

The DCN is routinely required to hold the following personal data where relevant:

- Name, home and work address and telephone numbers
- Email address
- Service number and rank
- Marital status
- Gender
- Date of birth
- Date of joining

- Details of minors for any regular medication if relevant (e.g. for Easter Campers)
- Church affiliation and Christian experience (where relevant e.g. for Trustees)
- References for staff/ DCN post holders
- Copies of DBS certificates in line with Safeguarding Policy (where relevant)
- Job title and National Insurance number (staff only)
- Start date/salary at start date (staff only)
- Bank details (staff only)
- Next of kin and contact details (staff only)
- Details of pension schemes (staff only)
- Career history/previous employment (staff only)
- Qualifications obtained/membership of professional bodies (staff only)
- Appraisals (staff only)

Data held may be used for statistical analysis, e.g. to improve the benefit for future members.

Sensitive Personal Data

Sensitive personal data is information relating to a living individual who can be identified from the data which includes an expression of opinion about the individual.

Exceptionally the DCN may hold the following sensitive personal data to fulfil its role effectively (e.g. pertaining to a staff member. Under GDPR Sensitive Personal Data is defined as information consisting of:

- racial or ethnic origin
- political opinions
- religious or philosophical beliefs
- trade union membership
- genetic data
- biometric data
- data concerning health
- data concerning a natural person's sex life or sexual orientation
- other information of a personal nature

In order to process these types of data, consent from the data subject **must** be obtained by the DCN when handling the data. **Explicit consent must be given when it is sensitive personal data**. For example, to hold details of unspent criminal convictions of DCN members currently serving custodial sentences in prison. Spent (i.e. rehabilitated) convictions should not be recorded for reasons of rehabilitation with the exception of persons listed on the Sex Offenders Register which is important for safeguarding children and adults with social care needs.

Subject Access Requests (SAR)

All individuals who are the subject of personal data held by the DCN are entitled to:

- Ask what information the DCN holds about them and why
- Ask how to gain access to it
- Be informed how to keep it up to date
- Be informed about how the DCN is meeting its data protection obligations

SARs should be made by email to the DCN office@afcu.org.uk. They will be passed to the Operations Director for action.

Individuals may be charged £10 per subject access request. The Operations Director will aim to provide the relevant data within 14 days. It MUST be provided within 30 days. The DCN will always verify the identity of anyone making a SAR before handing over information.

If a SAR is denied by DCN, a reason for doing so must be supplied to the applicant within one month. They have the right to complain to the supervisory authority and to a judicial remedy.

Procedures relating to the Historical Record of DCN members

In addition to providing pastoral and prayer support, fellowship, discipleship and encouragement of members, the DCN maintains a historical record of members (some records dating back to 1851).

While it can be desirable to retain these records as part of the DCN's history, this is subject to the normal rights of data subjects (or their relatives if deceased) as explained in sections 10 - 12 of the policy above. These are:

- Right to be informed about the collection and use of their personal data
- Right of access to any data held about them by a data controller (see also clause 11)
- Right to rectification (see also clause 12)
- Right to erasure (see also clause 12)
- Right to restrict processing (see also clause 12)
- Right to data portability (see also clause 12)
- Right to object (see also clause 12)

Historical Records of Ex-members, Trustees and Staff Members

The normal approach, consistent with the data retention schedule, is that only essential records should be retained. Unless there is legislation to the contrary or e.g. a criminal/ safeguarding matter involved, the records of ex-members, trustees and staff members should normally be retained for no longer than six years which is the maximum legal limitation period for some types of claims (contractual, damage suffered, etc).

Subject to the timelines stated within the retention schedule, all non-essential details should be erased as followed:

- Within six months of a member leaving (who has not served in any significant role such as leadership or as a trustee)
- Within one year of a member leaving (if they served in any significant role such as leadership or as a trustee)
- Within one year of a staff member leaving

A record may be deemed to be "essential" if, for instance, it might be potentially relevant to a future legal claim. For example:

- Details of events attended and activities participated in
- Emails/ letters expressing concern or complaint (or appreciation)
- Concerns about an ex-member raised by another person which may be relevant to the claim of an existing member or other third party

After the expiry of six years (or other specified period), all records should be deleted with the exception of the following basic details which may legitimately form part of the DCN's historical record of membership:

- Name
- Dates of membership (when joined and left)
- Final rank /Service if applicable
- Date of birth (to identify in case of multiple persons of the same name)

The exception to this is if the person has sought to exercise the GDPR right of erasure, namely the "right to be forgotten" in which case all details apart from anything which must be retained for e.g. legal reasons must be deleted.

DCN members who withdraw their membership from DCN have a right to their personal details being deleted. This includes everything except the following information which is needed to maintain the historical record:

- Name
- Dates of membership (when joined and left)
- Final rank/Service if applicable
- Date of birth (to identify in case of multiple persons of the same name)
- Reason for withdrawal from membership

Historical Records of Deceased Members

The GDPR only applies to information which relates to an identifiable living individual. Information relating to a deceased person does not constitute personal data and therefore is not subject to the GDPR. Therefore, technically the DCN can hold any data it considers relevant and appropriate regarding deceased DCN (or OCU) members as part of its historical record. That said, discretion should be exercised in what and how much is held, especially since the deceased person is unable to e.g. rectify inaccurate or negative records about them. Family members have a right to see the information held by submitting a Subject Access Request.

APPENDIX 4: Data Protection Checklist

Existing Data

- Are you currently holding any personal data?
- Is it held securely?
- For what purpose are you holding it?
- Is it sensitive personal data? Do you have permission from the subject to hold it?
- Does the individual know you are holding their personal data/ have they given their consent?
- Has the DCN notified the Data Protection Commissioner that it holds this data and the purpose for which it is held?
- Is the data accurate?
- Does the data still need to be held?

New Data

- Make sure you include reference to the DCN Data Protection Policy on the form together with a relevant opt out for other communications
- When collecting data from new contacts by phone, email, or letter, make sure that they know about our data protection statement and email statement
- When requesting a new page to be put on the website that will result in the collection of data ensure that the page contains a link to the DCN's Privacy Statement, Data Protection Policy
- Delete the data when it is no longer required
- Don't take personal data from another organisation without the consent of the individual concerned

Using Data

- Are you passing personal data to anyone else?
- Inside the DCN
- Outside the DCN
- Are you using blind copies when sending email distribution lists?
- Is there a confidentiality agreement in place where it is necessary to pass data to a permitted third party?
- Do not pass personal data to any person outside of the DCN without the permission of the individual