New Barn
Christian Fellowship

NBCF
Data Protection Policy

New Barn Christian Fellowship

TABLE OF CONTENTS

1. Document Control

1.1. Issuer Details

Issuer	New Barn Christian Fellowship
Address	Scout Hall, Nurstead Lane, Longfield Hill, Longfield, DA3 7AN
Author(s)	Rowan Troy
Reviewer(s)	Ron Owen

1.2. Change History

Version	Date	Changes Made	Author/Editor	Approved By
0.1	01/03/2021	Draft	Rowan Troy	Ron Owen
1.0	05/04/2021	Release	Rowan Troy	Ron Owen

1.2.1. This is a CONTROLLED document. It is UNCONTROLLED when printed. You should verify that you have the most current issue.

2. Introduction

2.1.1. New Barn Christian Fellowship (known as NBCF from here on in) obtains, keeps and uses certain personal data about individuals. These can include members, suppliers, business contacts, employees, job applicants and other people the organisation has a relationship with or may need to contact.

2.1.2. This data protection policy ensures NBCF:

- Complies with data protection law and follows good practice;
- Protects the rights of staff, members, partners and other individuals;
- Is open and transparent about how it stores and processes individuals' data;
- Protects itself from the risks of a data breaches.

2.2. Purpose

2.2.1. The purpose of this policy is to describe how this personal data is collected, handled and stored to meet NBCF's data protection standards and to comply with the law.

2.3. Scope

2.3.1. This policy applies to:

- The Scout Hall notice board for NBCF;
- All current and former employees of NBCF;
- All contractors, suppliers and other people working on behalf of NBCF;
- Job applicants.

2.3.2. This Policy applies to all data that the company holds relating to identifiable individuals, in line with the Data Protection Act 2018 and the General Data Protection Regulation 2016/679. This can include:

- Names of individuals;
- Postal addresses;
- Email addresses;
- Telephone numbers;
- Photographs
- Digital video media
- Any other information relating to individuals who can be directly or indirectly identified from that information (including employment applications, references, bank details, and remuneration details).

2.3.3. This Policy applies to data that belongs to NBCF (for which we are the Data Controller), or data that belongs to members as a Data Processor).

2.4. DPO

2.4.1. NBCF has appointed Rowan Troy as the Data Protection Officer (DPO).

2.5. Review and Development

2.5.1. This policy shall be reviewed and updated as necessary by the NBCF Data Protection Officer to ensure its compliance with any changes to the law, organisational policies or contractual obligations.

3. Policy

3.1. Principles

3.1.1. NBCF commits to comply with the following principles when processing personal data:

- Personal data will be processed in a lawful, fair and transparent manner;
- Personal data will be processed only for the purpose for which they have been collected;
- Only personal data that is adequate, relevant and necessary in relation to the purpose will be processed;
- Every reasonable step will be taken to ensure that personal data is accurate and, if necessary, up to date;
- Personal data will be retained for no longer than necessary in relation to their purpose;
- Appropriate measures will be taken to ensure the security of personal data, including the protection against unauthorised and/or unlawful processing and the protection of its integrity and confidentiality.

3.2. Basis for Processing Personal Data

3.2.1. NBCF shall review the processing activities prior to the collection of personal data and for each of them shall select the most appropriate lawful basis for processing the data.

3.2.2. Processing is considered lawful to the extent that one of the following applies:

- The data subject has given consent to the processing of personal data for one or multiple specific purposes;
- The data subject is party to a contract which performance requires the processing of data or the processing is necessary to take steps at the request of the data subject prior to entering into a contract;
- The processing is necessary for compliance with a legal obligation to which NBCF is subject;
- The processing is necessary for the protection of the vital interests of the data subject or of another natural person;
- The processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority;
- The processing is necessary for the purpose of legitimate interest pursued by the controller or by a third party, when such interest is not overridden by the interest of fundamental rights and freedoms of the data subject.

3.2.3. More information can be found in NBCF Lawfulness of Processing Policy.

3.2.4. All the processing activities undertaken by NBCF are logged in the Data Protection Central Register.

3.3. The General Data Protection Regulation (GDPR)

3.3.1. The General Data Protection Regulation is underpinned by some important principles. According to these principles, personal data must:

- Be processed fairly, lawfully and in a transparent manner;
- Be obtained only for specified, explicit and legitimate purposes;
- Be adequate, relevant and limited to what is necessary in relation the purpose for which they are processed;
- Be accurate and, when necessary, kept up to date;
- Kept in a form that permits the identification of data subjects for no longer that necessary in relation to the purpose for which they are processed;
- Processed in a manner that ensures appropriate security;
- Not be transferred to a third country or to an international organisation, unless the conditions laid down in the GDPR are complied with by that country or organisation.

3.4. Data Protection Law and Data Quality

3.4.1. The Data Protection Law describes how organisations (including NBCF) must collect, handle and store personal information.

3.4.2. These rules apply regardless of whether data is stored electronically, on paper or on other materials.

3.4.3. To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

3.4.4. Data will be collected, stored and used in a manner that ensures it is relevant, timely, accurate, coherent, transparent and accessible.

3.4.5. NBCF adopts an approach to ensure all information is:

- Held securely and confidentially;
- Collected fairly and lawfully;
- Recorded accurately and reliably;
- Used effectively and ethically; and
- Shared appropriately and legally.

3.4.6. All information processed by NBCF will be handle according to best practices and aligned to industry and legal standards.

3.4.7. Good quality data should have the following characteristics:

- Accuracy – Data should have enough details to provide an accurate representation of the relevant activity;
- Validity – Data should be recorded in a way that ensures integrity and consistency;
- Timeliness – Data should be collected and recorded as quickly as possible and be retained for an agreed time period;
- Relevance – Data should be relevant and proportionate in relation to the purpose for which it is used;
- Completeness – Data should be complete and not contain redundant records.

3.5. Data Protection Risks

3.5.1. This policy helps to protect NBCF from some very real data security risks, including:

- Breaches of confidentiality (e.g. information being given out inappropriately);
- Failing to offer choice (e.g. all individuals shall be free to choose how the organisation uses data relating to them);
- Reputational damage (e.g. the organisation could suffer if hackers successfully gained access to sensitive data).

4. Rights of Data Subjects

4.1.1. All individuals who are the subject of personal data held by NBCF are entitled to:

- Be informed about how, why and on what basis their information is processed;
- Ask how to gain access to it;
- Have their data corrected or updated;
- Be informed how the company is meeting its data protection obligations;
- Have their data deleted if:
  - The data is no longer necessary for the purpose for which it was originally collected and processed;
  - The consent is withdrawn by the data subject;
  - The data subject exercises his right to object;
  - The data is being unlawfully processed;

- The data has to be erased for compliance with a legal obligation.

4.1.2. NBCF aims to ensure that individuals are aware that their data is being processed and that they understand:

- How the data is being used;
- How to exercise their rights.

4.1.3. To these ends, NBCF maintains a privacy statement setting out how data relating to individuals is used by the organisation. This can be viewed on the company's website.

4.2. Subject Access Requests

4.2.1. The right of data subjects to access their personal information is commonly referred to as subject access.

4.2.2. The purpose of the right of access is to allow individuals to verify the lawfulness of processing of personal data.

4.2.3. Subject access requests from individuals shall be made by email to Alan Murphy, Pastor of NBCF – alan.murphy90@outlook.com.

4.2.4. All the subject access requests will be handled according to the NBCF Subject Access Request Procedure.

4.3. Exemptions to Rights of Data Subjects

4.3.1. Personal data can be disclosed to competent authorities without the consent of the data subjects when such data must be processed for criminal law enforcement purposes.

4.3.2. The processing of personal data without consent is also allowed:

- For the purpose of safeguarding national security or for defence purposes, and
- With appropriate safeguards, for the rights and freedom of the data subject.

4.3.3. Under these circumstances, NBCF shall disclose the requested data. However, the DPO shall ensure the request is legitimate, seeking assistance from the Eldership and Trustee teams and from the company's legal advisers where necessary.

5. Obligations

5.1. Specific Obligations

5.1.1. Everyone who works for or with NBCF has some responsibility for ensuring data is collected, stored and handled appropriately.

5.1.2. Each individual that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles. However, there are key area of responsibilities.

5.1.3. The Trustees are ultimately responsible for ensuring that NBCF meets its legal obligations.

5.1.4. The Data Protection Officer is responsible for:

- Keeping the Eldership and Trustees updated about data protection responsibilities, risks and issues;
- Reviewing all data protection procedures and related policies, in line with an agreed schedule;
- Arranging data protection training and advice for the people covered by this policy;
- Handling data protection questions from staff and anyone else covered by this policy;
- Dealing with subject access requests;
- Checking and approving any contracts or agreements with third parties that may handle the organisation's sensitive data.

5.2. Individual Obligations

5.2.1. Individuals are responsible for communicating with the organisation and helping it keep their personal data up to date. If any personal data provided changes in the course of the employment or engagement, or if access is gained to new personal data, such changes should be promptly communicated to the DPO via telephone, email or post.

5.2.2. The only people able to access data covered by this policy shall be those who need it to support the work of NBCF.

5.2.3. Data shall not be shared informally. When access to confidential information is required, all requests must be communicated to the Eldership or Trustees prior to release.

5.2.4. NBCF shall provide training to all employees and those who support the work of NBCF to help them understand their responsibilities when handling data.

5.2.5. Employees, and those who support the work of NBCF, shall keep all data secure, by taking sensible precautions and following the guidelines below:

- Strong passwords must be used, and they shall never be shared;
- Personal data shall not be disclosed to unauthorised people, either within the organisation or externally;
- Data shall be regularly reviewed and updated if it is found to be out of date. If no longer required, it shall be deleted;
- Any individual shall request help from the DPO if they are unsure about any aspect of data protection.

6. Storage and Retention of Personal Data

6.1. Recruitment Process

6.1.1. During the recruitment process, the DPO will ensure that:

- No questions relating to sensitive personal information are asked during the interview and decision-making stage;
- If personal information is provided by the candidates without being asked, no record is kept and any reference to it is immediately deleted or redacted;
- The candidates' right to work is checked before any unconditional offer of employment is made.

6.2. Data Storage

6.2.1. These rules describe how and where data shall be safely stored. Questions about storing data safely can be directed to the DPO.

6.2.2. When data is stored on paper, it shall be kept in a secure place where unauthorised people cannot see it and it should not be left unattended.

6.2.3. These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper or files shall be kept in a locked drawer or filing cabinet;
- Employees, and those who support the work of NBCF, shall make sure paper and printouts are not left where unauthorised people could see them;
- Data printouts shall be shredded and disposed of securely when no longer required.

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

6.2.5. Data shall be protected by strong passwords that are changed regularly or protected with multifactor authentication and never shared.

6.2.6. If data is stored on removable media (like a CD, DVD), these shall be kept locked away securely when not being used.

6.2.7. Data shall only be stored on designated drives and cloud services and shall only be uploaded to an approved location by the DPO.

6.2.8. Data shall be backed up frequently. Those backups shall be tested regularly to ensure restoration is possible.

6.2.9. All servers and computers containing data shall be protected by appropriate means such as encryption and password protected storage.

6.2.10. Data is retained in accordance with the General Data Protection Regulation.

6.3. Data Use

6.3.1. When working with personal data, employees, and those who support the work of NBCF, shall ensure the screens of their computers are always locked when left unattended.

6.3.2. Personal data shall not be shared informally. It shall never be sent via email as this form of communication is not secure.

6.3.3. Data must be encrypted before being transferred electronically. The DPO can explain how to send data to authorised external contacts.

6.3.4. Personal data cannot be transferred outside the UK without the express permission of the DPO.

6.3.5. Employees, and those who support the work of NBCF, shall ensure any personal data stored on personal devices to appropriately secured with controls such as passwords/passphrases, pin codes, and encryption (either inherent or applied).

6.4. Data Accuracy

6.4.1. The law requires NBCF to take reasonable steps to ensure data is kept accurate and up to date.

6.4.2. Data shall be held in as few places as necessary. Individuals shall not create any unnecessary additional data sets.

6.4.3. Employees, and those who support the work of NBCF, shall take every opportunity to ensure data is updated. NBCF shall send a consent form at least annually to request updated contact details and consent.

6.4.4. NBCF shall make it easy for data subjects to update the information the organisation holds about them. For instance, via email or telephone.

6.4.5. Data shall be updated as inaccuracies are discovered.

7. Data Protection Impact Assessment (DPIA)

7.1.1. NBCF commits to collect and process personal data in compliance with the Data Protection Legislation and only when an appropriate lawful basis applies in accordance with the Lawfulness of Processing Policy. In certain cases, this will mean carrying out a Data Protection Impact Assessment (DPIA).

7.1.2. NBCF carries out DPIAs to systematically and comprehensively analyse any new project involving the processing of personal data and to minimise any risk related to it.

7.1.3. DPIAs consider compliance risks, but also broader risks to the rights and freedoms of individuals, including the potential for any significant social or economic disadvantage.

7.1.4. DPIAs must be reviewed, quality assured, approved and signed off by the Eldership and/or Trustees. The Data Controller is ultimately responsible for ensuring that the DPIA is carried out appropriately.

8. Data Breaches

8.1.1. Personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

8.1.2. If a data breach eventuates, NBCF may be obliged to take the following steps:

- Notify the Information Commissioner's Office without undue delay and, where feasible, no later than 72 hours after becoming aware of a breach when this is likely to result in a high risk to the rights and freedoms of individuals;
- Notify the affected individuals without undue delay if the breach is likely to result in a high risk to their rights and freedoms.

8.1.3. If there is a potential breach related to client data, NBCF may be obliged to inform its members without undue delay. Any potential breach must be escalated to the DPO to be dealt with appropriately.

9. Data Protection by Design and Default

9.1.1. NBCF commits to consider data protection issues during the early design and implementation stage of every new system or practice.

9.1.2. NBCF shall, where possible, implement appropriate technical and organisational measures, such as pseudonymisation and data minimisation, in order to protect the rights of the data subjects.

9.1.3. NBCF will process, by default, only the minimum amount of personal data necessary for the specific purpose it was originally collected and will ensure that the accessibility to this data is limited in order to minimize the impact on the data subjects' privacy.

9.1.4. NBCF commits to adopt a privacy by design approach that promotes data protection compliance from the start. For example, when:

- Building new IT systems for storing or accessing personal data;

- Developing legislation, policy or strategies that have privacy implications;
- Embarking on a data sharing initiative; or
- Using data for new purposes.

9.1.5. Taking a privacy by design approach is an essential tool in minimising privacy risks and building trust. Designing projects, processes, products or systems with privacy in mind at the outset can lead to benefits which include:

- Potential problems are identified at an early stage, when addressing them will often be simpler and less costly;
- Increased awareness of privacy and data protection across the organisation;
- Organisations are more likely to meet their legal obligations and less likely to breach the General Data Protection Regulation;
- Actions are less likely to be privacy intrusive and have a negative impact on individuals.

9.1.6. Privacy and data protection issues should be considered during the design phase of any system, service, product or process and then throughout the lifecycle.

9.1.7. Data Protection Impact Assessments (DPIAs) are an integral part of taking a privacy by design approach. DPIAs are a tool that can be used to identify and reduce the privacy risks of projects. A DPIA can reduce the risks of harm to individuals through the misuse of their personal information. It can also help to design more efficient and effective processes for handling personal data.

9.1.8. Data protection by design is a broader concept as it applies organisationally and before deciding whether is appropriate to undertake a DPIA. However, DPIAs are important tool that can help in the identification and mitigation of data protection related risks.

9.2. Responsibilities and Risk Ownership

9.2.1. Notwithstanding the DPO responsibility of advising on data protection legislation and compliance risk mitigation, ultimately the risks belong to the Trustees.

9.2.2. In order to meet the above characteristics, all employees, and those who support the work of NBCF, are responsible for ensuring that data are:

- Collected accurately and recorded as soon as possible at the time of collection;
- Collected in accordance with any relevant standards and procedures;
- Updated in accordance with any relevant standard and procedures;
- Corrected in a timely basis.

9.2.3. All employees shall be made aware of the importance of good data quality and their own contribution to achieving it and shall receive appropriate training in relation to data quality aspects of their work.

9.2.4. All employees, and those who support the work of NBCF, shall communicate any issues with systems that are used to collect data and/or highlight and identified improvements to data source.

10. Enforcement

10.1.1. All individuals should be aware that they can be considered personally liable if they knowingly or recklessly disclose personal information outside the organisation's policies and procedures with possible penalties of large fines or imprisonment. It is a duty of every individual to familiarise themselves with this policy and apply it to their day to day activities.

11. Appendix I – Definitions and Acronyms

Personal Data	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.
Processing	Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Consent	Any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.
DPIA	Data Protection Impact Assessment
SAR	Subject Access Request