Data Protection and Information Security Policy

1. Introduction

Birmingham Vineyard needs to collect and use certain types of information about the individuals, volunteers or employees who come into contact with Birmingham Vineyard, in order to carry on our work. This personal information must be collected and dealt with appropriately whether collected on paper, stored in a computer database, or recorded on other material and there are safeguards to ensure this under the General Data Protection Regulation (GDPR).
This Policy Document encompasses all aspects of security surrounding confidential information including church members, suppliers, volunteers and employee data. This Policy is distributed to all employees and office volunteers. All employees/ volunteers must read this document in its entirety and sign the form confirming they have read and understand this policy fully.

2. Data Controller

Birmingham Vineyard is the Data Controller under the regulation, which means that it determines what purposes personal information held will be used for. It is also responsible for registration with the Information Commissioner and notification of the data it holds or is likely to hold, and the general purposes that this data will be used for.

3. Disclosure

Birmingham Vineyard may share data with other agencies in order to fulfil its contracts such as employer insurers and also with others such as the local authority or government agencies for lawful reasons.

The individual will be made aware in most circumstances how and with whom their information will be shared. There are circumstances where the law allows Birmingham Vineyard 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/employee/volunteer or other person;
- The individual/employee/volunteer 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/employee/volunteer'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 individual/employee/volunteer to provide consent signatures.

Birmingham Vineyard regards the lawful and correct treatment of personal information as very important to successful working, and to maintaining the confidence of those with whom we deal.

Birmingham Vineyard intends to ensure that personal information is treated lawfully and correctly.

To this end, Birmingham Vineyard will adhere to the Principles of General Data Protection Regulation.

Specifically, the Principles require that personal information is:

a) Processed lawfully, fairly and in a transparent manner in relation to individuals;
b) Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
c) Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
d) Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
e) 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; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
f) Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Birmingham Vineyard will, through appropriate management and strict application of criteria and controls:

a) Observe fully conditions regarding the fair collection and use of information;
b) Meet its legal obligations to specify the purposes for which information is used;
c) Collect and process appropriate information, and only to the extent that it is needed to fulfil its operational needs or to comply with any legal requirements;
d) Ensure the quality of information used;
e) Ensure that the rights of people about whom information is held, can be fully exercised under the Regulation. These include:
    - The right to be informed
    - The right of access
    - The right to rectification
    - The right to erasure
    - The right to restrict processing
    - The right to data portability
    - The right to object
    - Rights in relation to automated decision making and profiling.
f) Take appropriate technical and organisational security measures to safeguard personal information;
g) Ensure that personal information is not transferred abroad without suitable safeguards;
h) Treat people justly and fairly whatever their age, religion, disability, gender, sexual orientation or ethnicity when dealing with requests for information; and
i) Set out clear procedures for responding to requests for information.

4. Data Collection and Information Security

Birmingham Vineyard will ensure that data is collected within the boundaries defined in this policy. This applies to data that is collected in person and completing a form (online or in person) or purchasing tickets from our events section. This information and data must have robust safeguards in place to protect them, to protect individual's privacy, to ensure compliance with various regulations (including the General Data Protection Regulations, coming into force May 2018) and to guard the future of the charity.

When collecting data, Birmingham Vineyard will ensure that the employee/ volunteer/church member:

a) Clearly understands why the information is needed;
b) Understands what it will be used for and what the consequences are should the individual decide not to give consent; and
c) Has received sufficient information on why their data is needed and how it

will be used.

Birmingham Vineyard commits to respecting the privacy of all its church members, suppliers, volunteers and employees and to protecting any data about these from outside parties. To this end management are committed to maintaining a secure environment in which to process information/data so that we can meet these promises.

Employees should ensure that they:

- Handle employee, supplier, volunteer and church member information in a manner that fits with its sensitivity;
- Limit personal use of Birmingham Vineyard information and telecommunication systems and ensure it doesn't interfere with your job performance;
- Do not use e-mail, internet and other Charity resources to engage in any action that is offensive, threatening, discriminatory, defamatory, slanderous, pornographic, obscene, harassing or illegal;
- Do not disclose personal information unless authorised;
- Keep passwords and accounts secure;
- Do not install unauthorised software or hardware, including modems and wireless access unless you have explicit management approval;
- Always leave desks clear of sensitive data and lock computer screens when unattended;
- Information security incidents must be reported, without delay, to your line manager.

We each have a responsibility for ensuring our organisation's systems and data are protected from unauthorised access and improper use. If you are unclear about any of the policies detailed herein you should seek advice and guidance from your line manager.

Birmingham Vineyard reserves the right to monitor, access, review, audit, copy, store, or delete any electronic communications, equipment, systems and network traffic for any purpose.

5. Acceptable Use Policy

Intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to Birmingham Vineyard's established culture of openness, trust and integrity. Management is committed to protecting the employees, trustees and Birmingham Vineyard from illegal or damaging actions by individuals, either knowingly or unknowingly.

- Employees/volunteers are responsible for exercising good judgment regarding the reasonableness of personal use.
- Employees/volunteers should ensure that they have appropriate

credentials and are authenticated for the use of technologies.

- Employees/volunteers should take all necessary steps to prevent unauthorised access to confidential data.
- Employees/volunteers should ensure that technologies should be used and setup in acceptable network locations.
- Keep passwords secure and do not share accounts.
- Authorised users are responsible for the security of their passwords and accounts.
- All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature.
- Because information contained on portable computers is especially vulnerable, special care should be exercised.
- Employees/volunteers must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.
- Escalate any breach of confidential information to your line manager immediately.

6. Data Breach

In line with General Data Protection, Birmingham Vineyard will inform the ICO within 72 hours about any data breach. If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, Birmingham Vineyard and its operational team will also notify its trustees within the same timeframe.

7. Disciplinary Action

Violation of the standards, policies and procedures presented in this document by an employee will result in disciplinary action, from warnings or reprimands up to and including termination of employment. Claims of ignorance, good intentions or using poor judgment will not be used as excuses for non-compliance.

8. Information Classification

Data and media containing data must always be labelled to indicate sensitivity level:

Confidential data might include information assets for which there are legal requirements for preventing disclosure or financial penalties for disclosure, or data that would cause severe damage to Birmingham Vineyard if disclosed or modified. **Confidential data includes church member data**.

Internal Use data might include information that the data owner feels should be protected to prevent unauthorised disclosure.

Public data is information that may be freely disseminated.

Personal data means data that relates to a living individual who can be identified -

a) From the data, or
b) From the data and other information which is in the possession of, or is likely to come into the possession of, the data controller,
c) And includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

Sensitive personal data means personal data consisting of information as to:

a) the racial or ethnic origin of the data subject,
b) age,
c) political opinions,
d) religious beliefs or other beliefs of a similar nature,
e) whether they are a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992),
f) physical or mental health or condition,
g) sexual life,
h) gender and sexuality,
i) the commission or alleged commission by them of any offence, or
j) any proceedings for any offence committed or alleged to have been committed by them, the disposal of such proceedings or the sentence of any court in such proceedings.

9. Physical Security

Access to sensitive information in both hard and soft media format must be physically restricted to prevent unauthorised individuals from obtaining sensitive data.

- Employees/volunteers are responsible for exercising good judgment regarding the reasonableness of personal use.
- Employees/volunteers should ensure that they have appropriate credentials and are authenticated for the use of technologies.
- Employees/volunteers should take all necessary steps to prevent unauthorised access to confidential data which includes card holder data.
- Employees/volunteers should ensure that technologies should be used and setup in acceptable network locations.
- Employees/volunteers are responsible to advise their line manager or alternative (should line manager not be available) of any suspected breaches of personal data immediately.
- A “visitor” is defined as a vendor, guest of an employee/volunteer, service personnel, or anyone who needs to enter the premises for a short duration, usually not more than one day.

- Keep passwords secure and do not share accounts. Authorised users are responsible for the security of their passwords and accounts.
- Media is defined as any printed or handwritten paper, received faxes, disks, memory sticks, computer hard drive etc.
- Visitors must always be escorted by a trusted employee/volunteer when in areas that hold sensitive information.
- Procedures must be in place to help all personnel easily distinguish between employees and visitors. “Employee” refers to full-time and part-time employees, temporary employees and personnel. A “visitor” is defined as a vendor, guest of an employee, service personnel, or anyone who needs to enter the premises for a short duration, usually not more than one day.
- Strict control is maintained over the storage and accessibility of media.

10. Disposal of Stored Data

- All data must be securely disposed of when no longer required by Birmingham Vineyard, regardless of the media or application type on which it is stored.
- An automatic process must exist to permanently delete on-line data, when no longer required.
- Birmingham Vineyard will have procedures for the destruction of hardcopy (paper) materials. These will require that all hardcopy materials are crosscut shredded, incinerated or pulped so they cannot be reconstructed.

11. Security Awareness and Procedures

The policies and procedures outlined below must be incorporated into charity practice to maintain a high level of security awareness. The protection of sensitive data demands regular training of all employees, volunteers and contractors.

- Review handling procedures for sensitive information and hold periodic security awareness meetings to incorporate these procedures into day to day charity practice.
- Distribute this policy document to all charity employees/volunteers to read. It is required that all employees/volunteers confirm that they understand the content of this security policy document by signing an acknowledgement form (see Appendix A).
- Charity security policies must be reviewed annually and updated as needed.

12. Remote Access policy

- It is the responsibility of Birmingham Vineyard employees, volunteers, contractors, vendors and agents with remote access privileges to Birmingham Vineyard’s corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to Birmingham Vineyard.

- Secure remote access must be strictly controlled. Control will be enforced by two factor authentication via one-time password authentication or public/private keys with strong pass-phrases.
- All hosts that are connected to Birmingham Vineyard internal networks via remote access technologies will be monitored on a regular basis.
- All remote access accounts used by vendors or third parties will be reconciled at regular interviews and the accounts will be revoked if there is no further business justification.
- Vendor accounts with access to Birmingham Vineyard network will only be enabled during the time period the access is required and will be disabled or removed once access is no longer required.

13. Review

13.1. This document will be reviewed where:

- There are newly developed security standards;
- Significant changes to legislation or regulations;
- There are found to be deficiencies or failures in this document, as a result of complaints or findings from any independent organisations at which point the lead officer will initiate an immediate review.

13.2. In any event this document and procedures will be reviewed annually by the trustees and revised as necessary.

Appendix One

Agreement to Comply Form

Agreement to Comply With Data Protection and Information Security Policies

_____

Employee/Volunteer Name (printed)

I agree to take all reasonable precautions to assure that internal information, or information that has been entrusted to Birmingham Vineyard by third parties such as church members, will not be disclosed to unauthorised persons. At the end of my employment, contract or time with Birmingham Vineyard, I agree to return all information to which I have had access as a result of my position. I understand that I am not authorised to use sensitive information for my own purposes, nor am I at liberty to provide this information to third parties without the express written consent of the Company Secretary who is the Designated Information Owner.

I have access to a copy of the Data Protection and Information Security Policy, I have read and understand these policies, and I understand how it impacts my job. As a condition of continued employment/volunteering, I agree to abide by the policies and other requirements found in this Birmingham Vineyard policy. I understand that non-compliance will be cause for disciplinary action up to and including dismissal, and perhaps criminal and/or civil penalties.

I also agree to promptly report all violations or suspected violations of information security policies to my line manager.

_____

Employee Signature

_____

Date

Appendix Two

Data Protection Procedures

Birmingham Vineyard Data Protection – Employee/Office Volunteer Guidelines

Sources:

- Information Commissioner's Office
- Uni of the West of England staff guidelines
- London School of Economics staff guidelines
- Anglia Ruskin University staff guidelines

Data Protection Officer: Company Secretary (Office Manager & PA)

This document provides Birmingham Vineyard employees/office volunteers with some general advice on Data Protection issues and the use of personal data.

What is Personal Data?

As a Birmingham Vineyard employee/office volunteer you may have access to a wide range of personal data. It can include (but is not limited to) names, phone numbers, address, date of birth, marital status, health information, financial information, bank details and even email addresses.

How should I store and use Personal Data?

Employees/office volunteers at Birmingham Vineyard are obliged to ensure that, if their job requires them to collect or use personal data about **church members** or **other employees**, records should be maintained so that they are:

- Accurate
- Up to date
- Fair (i.e. they are not used for purposes other than those for which the information was obtained and the subject of the information is not deceived in any way as to these purposes)
- Secure* (personal data which is physically held is kept securely and personal data is not disclosed either orally or in writing, accidentally or otherwise to any unauthorised party)
- Disposed of safely

* Secure storage does not mean that extreme security measures are required. Providing it is adequate for the data and environment, this should be sufficient. Simple 'adequate' storage can include (for paper records):

- A locked filing cabinet, or
- A locked drawer, or
- A locked office

For electronic records:

- Password protection on files and/or

- Locking the computer (Ctrl, Alt & Delete) when leaving the desk.

What do I do if I get a request for Personal Data?

All requests for information under the Data Protection Act 1998 from third parties should be passed in writing to the Company Secretary immediately. These could include requests from parents, the police, the UK Border Agency or other statutory authority. Please note that there is a very tight time limit in which to respond to these requests, so they should be passed on without delay. If the Company Secretary isn't available, contact the Chair of Trustees or Executive Pastor immediately.

- **Internal requests for personal information.**

Personal data ***can*** be passed internally between Birmingham Vineyard staff/volunteers if it is required to carry out our daily duties. Birmingham Vineyard is registered as one 'Data Controller' in accordance with the Data Protection Act 1998, therefore passing information internally does not qualify as 'disclosing' to a third party.
However, to avoid creating copies of personal data Birmingham Vineyard staff should, wherever possible, keep personal data in a central secure store (eg ChurchSuite) and access the necessary information there.

- **Requests from non-staff members**

Church Trustees, Community Leaders, Small Group Leaders and other leaders of ministries and teams in the church may request personal information. As above, this is not an external request. However, Birmingham Vineyard staff/volunteers are encouraged to check that the request is for a legitimate church purpose, and that the information is NOT stored/held by the individual, but is returned to Birmingham Vineyard, or securely destroyed.
It is extremely unlikely that any of the above non-staff members would have any legitimate church purpose for requesting personal financial information.

For any request, if you are unsure that it is appropriate, please refer to the Company Secretary.

Personal data on the internet

Birmingham Vineyard must abide by the 8th Data Protection Principle which states that personal data will not be 'transferred' beyond the European Economic Area to countries without data protection legislation. Any information published on our church website, our Facebook pages, Instagram or Twitter becomes accessible from anywhere in the world. It is therefore important to take great care when publishing to the worldwide web.
Where personal information is published on the web, explicit consent must be obtained.
Even where permission has been obtained, the data subject has the right to withdraw consent at any time.
When sending an email to a large number of people, please remember that an email address is also personal data – long lists should use the BCC function to avoid sharing addresses to all recipients, wherever possible.

Filming and photography

Anyone on church property or at a church event wishing to take photographs or make a film that will later be published (in any medium), must consider the environment they are working in and our safeguarding policies.

Production of Information Request Cards/Letters

For any form produced where information is requested, it is the employee's responsibility to include the following statement:

I give consent for Birmingham Vineyard to store my information for church purposes.
For more information on our Data Policy please see www.birminghamvineyard.com

Training and Support

If you have any questions, or require further Data Protection training, please contact the Company Secretary.