Data Protection *(from May 2108 is covered by)*

GENERAL DATA PROTECTION REGULATION (GDPR)

Issue: Version 1B

Classification: Internal use only

Document Owner: Board of Trustees

Original Author: S. Ward

Revised by: Mike Woodroof

This document replaces in whole, our previous Data Protection Policy, and is compliant with the General Data Protection Regulation which becomes law in May 2018

Registered Address: Hutton Community Centre, Harrison Close, Hutton, Brentwood, Essex, CM13 1LP
Registered Charity No. 1131190

History of Change

Version	Date	Description
	04/03/2013	First Draft
V1	29/04/2013	Changed draft to Version 1
V1A	01/08/2017	Revised H Gell
V1B	11/04/2018	Revised M. Woodroof

Contents

1. Purpose and Scope

This policy document applies to all members of, and those employed by, Hope Community Church, with the registered address of Hutton Community Centre, Harrison Close, Hutton, Brentwood, Essex, CM13 1LP ("the Organisation") and all other Organisation sites that they may visit from time to time.

2. Data Protection Principles

The Organisation complies with the General Data Protection Regulation ("GDPR") and the principles of the Act, your personal data will be:

1. Fairly and lawfully processed.
2. Processed for limited purposes and not in any way incompatible with those purposes.
3. Adequate, relevant and will not be excessive.
4. Accurate.
5. Not kept for longer than necessary
6. Processed in accordance with your individual rights.
7. Secure.
8. Not transferred to countries without adequate data protection.

3. Your Agreement

Those employed by the Organisation agree to collection and storage of their data under the GDPR. Members of the Organisation consent to their details being held by the Organisation, for the time they are a member of the organisation and they have the right to amend or delete it

. This data will also be published in the address book on our website which is only accessible to members who have so agreed.

Any member not wishing to have their details held by the Organisation; or published in the website address book should complete the relevant sections on form DP1 to request this.

4. Your Personal Data

The Organisation only holds personal data necessary to its efficient running. This will include Name, Address, Telephone, e-mail address. Those employed by the Organisation, will also have the following included:

a) Third-party employment references.
b) Employment reports or assessments, including performance reviews.
c) Disciplinary details, including informal or formal warnings.
d) Grievance procedures and outcomes.
e) Salary reviews, benefits records and expenses claims.
f) Health records.

This information is only collected to assist our admin department in the smooth running of the Organisation and to ensure that the Organisation complies with other statutory responsibilities.

Employees personal data may be disclosed within the Organisation to those within the personnel department and management, including their immediate manager. Such personal data will not be disclosed to your peers or any other employees that do not require access to the data in order to carry out their own roles within the Organisation.

5. Maintaining Records

The Organisation will take all reasonable steps to ensure that personal data held by the Organisation is accurate and kept up to date. To ensure accuracy the Organisation will ask employees and members every 12 months to check that their personal information held by the Organisation is correct. Employees and members should always contact the admin department should their personal information change for any reason, for example a change of surname, home address or telephone number. Out of date information or information that is no longer required will be deleted by the Organisation on a regular basis.

6. Sickness & Health Records

For day-to-day management, the Organisation needs to keep records relating to the personal sickness and health records of each employee. Such personal data will record any periods of sickness or health matters, detailing the length and nature of the issue and the outcome. These records will be used to assess the health and welfare of employees and to highlight any issues that may require further investigation. Such data will only be disclosed to management and will not be disclosed to fellow employees, (except those employees within the personnel department who process such data). If for any reason you do not wish your health records to be kept please contact your line manager or Chair of Trustees.

7. Security of Data

The Organisation is committed to the secure storage and where undertaken the secure transmission of members and employees' personal data. Only management and employees within the personnel department have access to such data. All such data is protected by physical security, such as locks and technical security, such as usernames and passwords to access computer records and data. Such data is only disclosed on a "need to know" basis. To further ensure the security of such records the Organisation reserves the right to monitor and keep detailed log file and computer data analysis of all accesses to employees' personal data. The Organisation also reserves the right to vet all employees who have access to such data in the course of their normal employment within the Organisation.

If you have legitimate access to personal data and you pass or transmit the data within the Organisation to another party or parties who in turn have the right to see such data, the following rules apply:

1. If the data is transmitted by email it must be sent in an encrypted form. The Hope e-mail system has been updated to run on encrypted servers which automatically add the disclaimer below and no e-mail containing information about members or staff which might infringe the GDPR should be transmitted from private e-mail addresses.

2. All e-mails will carry the following disclaimer:

   Hope Community Church are registered in England under Charity No. 1131190.
   Our registered office is: Hutton Community Centre, Harrison Close, Hutton, Brentwood, Essex, CM13 1LP.
   We are part of the Relational Mission Group of Churches (formerly New Frontiers)
   This e-mail (including any attachments) is intended only for the recipient(s) named above. It may contain confidential or privileged information and should not be read, copied or otherwise used by any other person unless express permission is given. If you are not a named recipient, please contact the sender and delete the e-mail from your system. It is the recipient's responsibility to ensure that appropriate measures are in place to check for software viruses. If you do not wish to receive e-mails in future from Hope Community Church contact our administrator.

3. If the data is transmitted via a network it must be done using a secure network. Wherever possible such data should not be sent via a wireless network where the risk of interception is greater.
4. Such data should not be kept within the email program on your PC after it has been sent or received. The data must be removed from the body of the email message or deleted from any temporary folders if sent as an attachment. Care should be taken at all times not to delete the original data source.
5. If the data is to be faxed ensure that the intended recipient knows in advance that the data is coming via fax and that they are standing by the fax machine to receive the data. Ensure that the fax number is correct. You should also confirm safe receipt of the data by the recipient.
6. If data is to be passed in hard copy form it should be handed to the recipient personally, the recipient should ensure that the data is stored in a locked drawer or cabinet.
7. Parties with legitimate access to such data should not use third parties without the authority to view the data to send or receive the data on their behalf.
8. All employees are reminded that unauthorised attempts to gain access to such data or accessing such data is a disciplinary offence and in certain situations may constitute gross misconduct leading to summary dismissal. Such breaches may also constitute a criminal offence under the General Data Protection Regulation.

8. External Data Processing

Where the Organisation uses third parties to process data and provide services or administer schemes around such data the Organisation will take reasonable steps to ensure that such third parties have in place their own data protection policies.

9. Benefits Schemes

Where the Organisation provides additional benefits such as health insurance and pension schemes the Organisation will not make use of data collected by third parties administering the schemes where such data is not required for the day-to day operation of the Organisation. The Organisation will provide employees with details of what information will be collected by these third parties and how it will be used. Furthermore, the Organisation will seek permission for the collection and use of this data prior to collection.

10. Equal Opportunities Monitoring

The Organisation may collect information relating to ethnic origin, sex or disability as part of an equal opportunities policy. The Organisation will ensure that any questionnaires relating to such information are accurate and that where possible the results will identify employment trends within the Organisation, and not identify individual employees.

11. Employee Reviews & Appraisals

The Organisation will only collect data required for employee review and appraisal that is necessary to facilitate this for the day-to day operation of the Organisation.

12. Data Transfers Outside the European Economic Area

If the Organisation transfers data outside the European Economic Area such data will only be transferred to countries deemed by the European Commission to provide adequate data protection or to countries, which are recognised "safe harbours" for such data. However, the Organisation may transfer data to other countries where the permission of the employees has been given.

13. Data Access & Disclosure

All prospective, current or past employees have the right to request access to data directly relating to them, which is held by the Organisation. The Organisation is entitled to seek a fee of up to £10 to deal with each request. Furthermore, the Organisation can request further information from the person making the request in order to provide accurate and relevant results and to check the identity of the person making the request. The Organisation seeks to provide such information within 40 days of receiving a request. The Organisation will provide the person making the request with the following information:

Whether they hold any information regarding them, and if they do:

1. Descriptions of that information
2. What it is used for.
3. The type of third party Organisations it is passed to.
4. Provide a breakdown of any technical terms or codes.

The information where reasonably possible will be provided in a hard copy or permanent electronic form.

14. References

The Organisation will not disclose details of confidential references where to do so would disclose the identity of the author or where it may cause harm or detriment to the author.

15. External Disclosure Requests

Where employees receive external requests for the disclosure of data the following guidelines should be observed:

1. Verify the identity of the person requesting the information.
2. Be on the lookout for fraud or deception.
3. Seek a written request where possible.
4. Check any telephone numbers where an oral request is received.
5. Inform the Chair of Trustees if any request appears suspicious.
6. The Chair of Trustees should also be contacted where the party requesting the data states that disclosure is required by law.
7. Remember that a duty is owed to the employee whose data is to be disclosed, where possible seek their permission, unless doing so would alert them to a criminal investigation.
8. If the disclosure of the data is non-routine where possible provide the employee in question with a copy of the data disclosed. A record of all non-routine data disclosures should also be kept.

16. Other Disclosures

Where the Organisation wishes to disclose employee data for promotional, marketing or other business purposes, (for example incorporated into an advertisement or brochure) the consent of the employee must be sought in advance. The employee should also be told where the data will be published and how widely.

17. Trade Unions

The Organisation will only provide data to trade unions where the trade union is recognised by the employer. The data will be limited to name, job description and job location. The Organisation will also give each employee a prior right to object to the disclosure. Where any such data is provided for collective bargaining the data will not identify individual employees.

18. Employee Monitoring

The Organisation will inform all employees where employee monitoring is introduced or increased. The Organisation will take reasonable steps to ensure that employee's privacy and autonomy are preserved. The Organisation will take reasonable steps to ensure that specific details of personal conversations or correspondence are not accessed. However, the Organisation retains the right to monitor the actual use of Organisation resources by employees.

19. CCTV Monitoring

The Organisation reserves the right to introduce or extend the use of CCTV within the Organisation's premises for security purposes. Where this occurs, signs will be displayed on the premises to make it clear to staff and visitors that CCTV is being used.

1. CCTV will only be used to monitoring activity on the Organisation's own premises.
2. Recorded images will be stored securely; with only authorised Organisation employees and (where requested) the police will have access to them.
3. Recorded images will only be retained for as long as necessary or where the police or courts require evidence.
4. All CCTV equipment will be regularly inspected to ensure proper functioning.

20. Medical Testing

If the Organisation undertakes any form of medical testing of employees such testing will only be undertaken for clear health and safety reasons, for assessing an employee's medical fitness for continued employment or to assess their entitlement to health benefits, such as sick pay. Prospective employees may be tested for similar reasons. The results of any testing required for a health or pension scheme shall not be given to the Organisation.

Retention of Employee Records
The Organisation will retain employee records for the following periods:

1. Application Form: for period of employment
2. References: 1 year
3. Payroll and tax information: 6 years
4. Sickness records: 3 years
5. Annual leave records: 2 years
6. Unpaid/special leave records: 3 years
7. Annual appraisal/ assessments: 5 years
8. Promotions: 1 year from end of employment
9. Transfers: 1 year from end of employment
10. Training: 1 year from end of employment
11. Disciplinary matters: 1 year from end of employment
12. References provided: 5 years from provided or end of employment
13. Summary of service: 10 years from end of employment
14. Injury or accident at work: 12 years from end of employment

The Organisation will ensure the safe and secure disposal of employee and members records that are no longer required.

21. Criminal Liability

Knowingly or recklessly disclosing the personal data of others without the express consent of the Organisation can constitute a criminal offence.

22. Date of Implementation

This policy is effective from May 25th, 2018 and shall not apply to any actions that occurred prior to this date.

23. Questions

If you have any questions regarding this policy document and how it applies to you, including how to request access to your personal data please consult the Chair of Trustees.

24. Alteration of this Policy

This policy will be subject to review, revision, change, updating, alteration and replacement in order to introduce new policies from time to time to reflect the changing needs of the business and to comply with legislation. Any alterations will be communicated to you by the Chair of Trustees.