HOPE into ACTION
NORTHUMBERLAND
Enabling churches to house the homeless

GDPR Policy & Procedures

Date Approved: 06/04/2020 *02/11/20*

Review before: 01/05/2021 *02/11/22*

Table of Contents

1. Introduction

We recognise that the correct and lawful treatment of personal data will maintain confidence in the organisation and underpin success in our mission. Protecting the confidentiality and integrity of personal data is a critical responsibility that we take seriously at all times.

The Data Protection Act 2018 and the General Data Protection Regulation came into force on 25th May 2018 and all personal data must be handled in accordance with its requirements. It applies to all data howsoever it is held about our past or present customers, tenants, supporters, investors, volunteers, employees, workers and other third parties or website users, or any other data subject.

Hope into Action UK is registered with the Information Commissioner (number is Z2945877). Further details of the Data Protection register entry can be found on the Information Commissioner's Office (ICO) website at http://www.ico.gov.uk/. Franchisees will need to register separately with the ICO. Hope into Action UK makes annual submissions to the ICO detailing the purposes for which personal information is processed; the types of individuals who are the subject of the data (data subjects); the types of data being processed (data classes); the individuals or organisations to which the Hope into Action does or intends to disclose data and the countries to which, if any, the data is transferred.

2. Security

- The Finance Director is appointed as Data Protection Officer and has responsibility for our data protection policy, procedures and compliance.
- We will regularly evaluate and test the effectiveness of our systems and processes to ensure security of our personal data and compliance with GDPR. Transmission of data across the internet is not completely secure and we will develop safeguards (including use of encryption and Pseudonymisation where applicable).
- A login account with password is required to access data held on our computer system and access to personal data restricted to those members of staff or volunteers whose job roles require such access.
- HiA staff and workers will not use their own personal email addresses for work. When mailing out to more than one recipient, other data subjects' addresses must not be revealed.
- There will be automatic time out /lock screen on all devices and access to data via secure Wi-Fi networks.
- Appropriate data is to be stored on to SharePoint and the paper then destroyed. If Sharepoint is not available then data should be saved to Microsoft One Drive. No personal data will be stored on an office PC or laptop, or on mobile devices or personal storage devices such as USB sticks and external hard drives.
- Papers are to be kept in a secure locked cupboard or secure locked room with the key only available to authorised members of staff.
- Email addresses for supporters who receive the HiA email newsletter are held on Mailchimp, (see Marketing below). However we retain control of the information.
- By completing the GDPR Checklist we will demonstrate compliance with these principles.

3.Training

HiA will arrange appropriate training (at induction of staff and at least annually) so that all personnel understand what is required in order to comply with GDPR and that any breaches by personnel may result in disciplinary action.

Training will be reported to trustees and monitored by them.

4.Governance

We will annually check that adequate governance and resources are in place to ensure proper use and protection of personal data. Ultimate responsibility for compliance rests with the Trustees.

5. Data Mapping

A data mapping exercise is to be carried out annually to document:

- what information we hold
- where it came from,

- Its purpose: how we process it and why we use it
- how and where it is held
- who we share it with including suppliers
- how long we retain
- Its source

6. Relevant personal data

Personal Data is any information identifying a Data Subject or information relating to a Data Subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access.

Personal Data includes Sensitive Personal Data and Pseudonymised Personal data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

7. Sharing Personal Data

Personal Data will be:

- Collected and processed lawfully and not used for any purpose other than that stated
- Relevant to the purpose and not excessive
- Accurate and kept up to date. Inaccuracies to be corrected or deleted without delay
- Only kept for as long as necessary or as required by law (the appropriate retention period). See section 13
- Kept confidential and only approved personnel can have access to it.
- Only transferred to third-party service providers who have a contract in place with us and comply with our required policies and procedures.
- If data has been sourced from a third party that source must be stated in the Privacy Notice.

8. Sharing Personal Data

- Generally we will not share personal data under any circumstances. Personal data may only be shared with another employee, agent or franchisee of HiA if the recipient has a job-related need to know.
- Data may be shared in the following examples:

i) where there is a statutory duty such as under the Landlord and Tenant Acts and under PAYE or criminal law requiring cooperation with the Police

ii) under contractual arrangements with tenants where data needs to be shared with utility companies and support agencies

- Personal data cannot be shared with third parties such as service providers unless certain safeguards and contractual arrangements have been put in place:

a) they have a need to know the information for the purposes of providing the contracted services

b) sharing the Personal Data complies with the Privacy Notice provided to the Data Subject

c) written contract in place whereby the third party has agreed to comply with the required data security standards, policies and procedures. Subcontracting is prohibited unless consent has been given

d) the transfer complies with any applicable cross border transfer restrictions

9. Privacy Notices (See Appendices 1-5)

Privacy notices will be published and updated annually for the Data Subjects listed below. The Supporter's Privacy Notice will be posted on our web site.

Whenever we collect Personal Data directly from data subjects, we will provide them with a relevant privacy notice confirming:

- HiA is the Data Controller (unless Joint Controller with the franchisee)
- The Data Privacy Officer is the Finance Director
- Our lawful basis
- Relevant personal data (listed above)
- Relevant information covered by data mapping (listed above)
- Right of erasure
- Right of complaint

10. HiA Lawful basis for processing personal data

GDPR provides for 6 lawful basis for processing personal data. It is essential we identify and document the legal ground being relied on for each processing activity. The lawful basis upon which we hold personal data for each category is as follows:

Data Subjects	**Lawful Basis**
Tenants	Performance of a contract*
Children under 13	Consent (by carer)
Referral Agencies	Performance of a contract
Employees	Performance of a contract
Volunteers	Performance of a contract
New Financial Donors	Consent
Investors	Performance of a contract
Historic Supporters & Donors	Legitimate Interest
Franchisees	Performance of a contract

* See the Tenant Privacy Notice for additional basis

10.1 Consent

- New supporters will have their personal data processed on the basis of consent. This requires completion by the supporter of the Data Consent Form (Appendix 9) or completing the opt-in box for email/phone/address on the web page.
- Carers of children under 13 will be required to give their consent to our holding their data.
- Consent requires affirmative action so silence, pre-ticked boxes or inactivity is unlikely to be sufficient.
- A privacy notice must be made available to the Data Subject at the time of consent and the purposes for which we process personal data is set out in this.
- A record of all consents will be kept so that the Company can demonstrate compliance with consent requirements.

10.2 Contract performance

Where individuals have requested a service such as our tenants, this creates a "performance of a contract" and as such HiA needs to process the personal data in order to comply with its obligations.

The personal data of employees such as payroll data and volunteers is also held under performance of contract and as such HiA needs to process the personal data in order to comply with its obligations.

10.3 Legitimate interest

The lawful basis for HiA holding and processing the personal data of existing supporters and donors is "legitimate interest". See Appendix 7 for our application of the required three part test:

1. Purpose test: are we pursuing a legitimate interest?

2. Necessity test: is the process necessary for that purpose?

3. Balancing test: do the individual's interests override the legitimate interest?

Our legitimate interests involve furthering our charitable objects of enabling churches to house the homeless through the information and services we provide and include our belief that prayer support is essential in achieving our charitable objectives. It benefits our tenants, keeps our supporters informed and engaged and has wider societal benefits.

The holding and processing of this data is necessary since without it our work would be unsustainable with finances, prayer support and volunteering all declining.

Relying on legitimate interests means we check that the processing of data will not cause harm and we will only hold personal data for the purposes and to process data in a way described in the Supporters Privacy Notice.

Holding and processing our existing supporters' and donors' personal data is of critical benefit to us and also offers great benefit to our existing supporters and donors. There are no obvious negative impacts and there are safeguards in place.

Newsletters or similar communications will always have an opt-out or "unsubscribe" option. If a supporter opts out at any time, the details will be suppressed as soon as possible. Suppression involves retaining just enough information to ensure that marketing preferences are respected in the future.

10.4 Legal compliance

Complying with a common law or statutory obligation. No personal data will be categorised under this basis as employee data (such as PAYE and Gift Aid) is processed under the basis of performance contract.

10.5 Vital interest

This relates to protecting life and no data under this basis will be held.

10.6 Public task

This relates to official processing and no data under this basis will be held.

11. Special Category Data

- Special category data covers data for example on a tenant's medication, drug abuse, physical and mental health, medical history, ethnicity, religion, and sexual preference.
- The data is held for the tenant's wellbeing and to facilitate appropriate services and support and for Health & Safety and for their vital interests all in accordance with HIA's safeguarding policy.
- The lawful basis for this, is that it is in the tenant's and our legitimate interest, and necessary for us to in order to perform our role. We check that the processing of special category data will not cause harm and we will only hold it and process it in for the purposes outlined here.
- We will hold and process data under the special category data consent provided: see Permission to Exchange Information Agreement

12 PECR

The Privacy & Electronic Communications Regulations (PECR) have applied since 2003 and restrict unsolicited marketing by phone, fax, email and text.

Our signup sheet has provided explicit consent for sending emails and Mailchimp has been used for all marketing emails including newsletters and annual reviews and has always included an unsubscribe option. All future communication with our supporters will continue to offer the right to object including an unsubscribe option.

Emailing news of events and activities has cultivated a committed community of supporters, unified in prayer with common cause and values.

In our judgement our supporters have given consent to receiving our marketing emails and we have a legal basis to continue sending these out.

Please see Appendix 7

13. Retention of Data

Data will be retained as follows:

	Retention period	Source
Audit		
Final reports	7 years after legal proceedings	Best practice
Other Audit reports and documents	6 years from completion	Best practice
Board		
Board minutes and papers	Permanent preservation	The National Archives
Other Board documents and details of appointments	6 years from creation	Best practice
Client/Customer Care		
Details of clients together with complaints, statistics and logs	Full file to be kept for 6months Abbreviated details indefinitely	Best practice
Finance		
Insurance – public liability policies, product liability policies, employers liability policies	40 years after the life of the organization	Best practice
Correspondence with Inland Revenue	Review every three years	Best practice
Internal correspondence	1 year	Best practice
All other financial records	7 years from creation	Tax Management Act 1970, The Limitation Act 1980, Value Added Tax Act 1994, Companies Act 1985
HR		
Job applications and interview records for unsuccessful applicants	6 months after notifying unsuccessful candidates	Sex Discrimination and Race Relations Act
Training History	2 years	Best practice
Current basic details (addresses etc)	Until superseded	Data Protection Act
Emergency procedures		
Pension details	Held by external pension provider	
All other HR documents	6 years after end of employment	Employment Relations Act, Sex Discrimination Act, Race Relations Act

IT		
Back up of email server	6 years	Best practice
User support	1 year	Best practice
Copy of website	Permanent preservation	The National Archives
All other files	6 years from creation	Best practice

Legal		
Records on establishment and development of the organization's legal framework and governance	Life of organization	Best practice
Legal grant file (Legal opinion, certificate of title, deeds of dedication etc)	Asset liability period	Best practice
Freedom of Information, Data Protection, Environmental Information Regulations. List of requests and responses, statistics, log	6 years from completion of request	Best practice
Litigation with third parties where legal precedents were set	Life of organization	The Limitation Act 1980
Litigation with third parties with no legal precedents	6 years after settlement of case	The Limitation Act 1980
Provision of Legal advice	6 years from date of advice	Best practice
Contracts and agreements	6 years from termination	The Limitation Act 1980
Unsuccessful tender documents	1 year after date of last paper	The Limitation Act 1980

Policy and Communications		
Details of events	3 years from creation	Best practice
All other documents	6 years from creation	Best practice

Projects		
Major Capital projects	At least 10 years	Best practice
All programs and project team documents	6 years from completion of project	Best practice

Team and Committee		
All minutes, papers, agendas and appointments	6 years from creation	Best practice

14. Data Subject's rights and requests

i. Data Subjects have rights when it comes to how we handle their personal data. These rights include:
ii. Where he/she has given consent, to withdraw consent at any time or restrict processing or access in specific circumstances
iii. request access to their personal data
iv. receive certain information about our processing activities and not be subject to automated decision-making including profiling
v. prevent our use of their personal data for direct marketing purposes and to challenge our legitimate interests
vi. ask us to erase personal data or rectify inaccurate or incomplete data
vii. data portability, that is data can be provided in a commonly used and machine-readable format. It relates solely to data originally provided by the data subject.
viii. be notified of a Personal Data Breach and to make a complaint to the ICO

Action Points

- The identity of an individual requesting data under any of the rights listed above must be verified and any data subject request immediately forwarded to the Data Protection Officer (dpo@hia.org.uk).
- If a supporter opts out at any time, the details will be suppressed as soon as possible. Suppression involves retaining just enough information to ensure that marketing preferences are respected in the future.

- In the event of an access request the information will be substantially provided within one month of the full request being received and in the case of a withdrawal of consent this should be actioned as soon as reasonably possible.
- In the event of us refusing a request we must give adequate reasons including:
    i. It would endanger an individual, render the data useless or seriously damage the reasons for its use
    ii. The information has been previously provided and nothing has changed
    iii. Either impossible to provide or requiring disproportionate effort
- This is to be noted on the tenant form.

15. Reporting a Personal Data Breach

- A personal data breach means a breach of security leading to the loss, alteration, unauthorised disclosure of or access to personal data, either accidental or deliberate. See under Definitions.
- If it is known or suspected that a personal data breach has occurred, the Data Protection Officer (dpo@hia.org.uk) should be immediately contacted, preserving all evidence relating to the potential breach. No attempt should be made to investigate the matter personally.
- We must notify any significant Personal Data Breach to the ICO within 72 hours and, if high risk, the Data Subject without delay. See Appendix 7 Data breach plan/flow-chart and Appendix 8 Data Breach Reporting & Register.
- Examples:
    - Disclosing other people's email addresses on a mail-out by failing to bcc
    - Under pressure from a family member, disclosing a data subject's address.
    - A laptop with unprotected personal data is stolen from a parked car

16. Changes to this Privacy Policy

We reserve the right to change this Privacy Policy at any time without notice so please check back regularly to obtain the latest copy.

Glossary of DEFINITIONS:

Company Personnel: all employees, workers, volunteers, contractors, agency workers, consultants, directors, members and others.

Consent: agreement which must be freely given, specific, informed and be an unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear positive action, signifies agreement to the processing of Personal Data relating to them.

Data Controller: the person or organisation that determines when, why and how to process Personal Data. It is responsible for establishing practices and policies in line with the GDPR. We are the Data Controller of all Personal Data relating to our Company Personnel and Personal Data used in our business for our own commercial purposes.

Data Subject: a living, identified or identifiable individual about whom we hold Personal Data. Data Subjects may be nationals or residents of any country and may have legal rights regarding their Personal Data.

Data Portability: allows individuals to obtain and reuse their personal data for their own purposes across different services. 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.

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

General Data Protection Regulation (GDPR): the General Data Protection Regulation (*(EU) 2016/679*). Personal Data is subject to the legal safeguards specified in the GDPR.

Personal Data: any information identifying a Data Subject or information relating to a Data Subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. Personal Data includes Sensitive Personal Data and Pseudonymised Personal Data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour. Personal Data specifically includes, but is not limited to this list.

Personal Data Breach: any act or omission that compromises the security, confidentiality, integrity or availability of Personal Data or the physical, technical, administrative or organisational safeguards that we or our third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of Personal Data is a Personal Data Breach.

Privacy Notices (also referred to as Fair Processing Notices) or Privacy Policies: separate notices setting out information that may be provided to Data Subjects when the Company collects information about them. These notices may take the form of general privacy statements applicable to a specific group of individuals (for example, employee privacy notices or the website privacy policy) or they may be stand-alone, one time privacy statements covering processing related to a specific purpose.

Processing or Process: any activity that involves the use of Personal Data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring Personal Data to third parties.

Pseudonymisation or Pseudonymised: replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person, to whom the data relates, cannot be identified without the use of additional information which is meant to be kept separately and secure.

Sensitive Personal Data: information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data, and Personal Data relating to criminal offences and convictions.

Appendices

1. Supporters Privacy Notice
2. Employees/Volunteers Privacy Notice
3. Tenant's Privacy Notice
4. Franchise Privacy Notice
5. Referral Agencies Privacy Notice
6. Data Breach Reporting & Register
7. Data Consent Form
8. Franchisor to Franchisee Data relationship – underlying principles
9. Summary of franchisee data processing