Inn Churches
The Storehouse, 116 Caledonia Street, Bradford, BD4 7BQ
hello@innchurches.co.uk | 01274 955010
www.innchurches.co.uk

Confidentiality and Data Protection Policy

Inn Churches recognises that any user of our services, whether an individual or an organisation, has the right to expect that information imparted by them to Inn Churches will be processed and stored securely, used only for the purpose for which it is given, and kept confidential.

Inn Churches is committed to the lawful and appropriate processing and storage of personal data, and the protection of that data when under our care.

Confidentiality

The right to privacy is essential to ensure that service users have trust and confidence in the organisation and are treated with respect and dignity. Information sharing sensitive information with Inn Churches have the right for it not to be released to anyone else without their consent.

We acknowledge that everyone involved with Inn Churches has a right to confidentiality.

Privacy by design

Inn Churches is committed to implementing processes and technologies to maintain confidentiality and to integrate data protection into all of the organisation's processing activities, including maintaining records of processing as required by Article 30 of GDPR.

The decision to introduce any new type of processing, particularly one using new technologies, will consider any potential risk to the rights and freedoms of individuals, and be the subject of a Data Protection Impact Assessment.

Processes

Personal and sensitive information held by Inn Churches, however obtained, will be processed in line with data protection law, and only in ways relevant to the purposes it was obtained for.

Access to the information held by Inn Churches will only be given to those with a genuine need to see and use it to deliver our services.

Inn Churches will ensure that all staff, contractors, volunteers and others working for or representing the charity understand their duties and responsibilities regarding confidentiality, including ensuring that they have read and agreed to this policy.

Information about the internal affairs of Inn Churches and its activities is confidential.

The Trustees will ensure that processes are in place to ensure that the minimal information needed to deliver the charity's services is collected, and that it is securely processed, stored and shared in line with published privacy notices.

Staff and volunteers must follow the principles and procedures in this policy to maintain the confidentiality and security of all records they make and hold, ensuring that information about others is accurate, up-to-date, and the minimum required to deliver their services.

Records must be kept securely, with access restricted only to those who need the information to carry out their duties.

Staff and volunteers will ensure that consideration is given to the physical environment in which information is gathered or shared and the method of sharing, including face-to-face discussions, telephone conversation, emails, and the use of scanner or copier. Care should be taken to ensure that confidential information cannot be overheard, overlooked or intercepted. In particular, personal details of service users will not be transmitted by email. Where service users need to be referred to, initials only should be used.

Information about service users should not be shared unnecessarily with other staff or volunteers, beyond what is needed to deliver the service.

When information is shared with other agencies, staff will ensure that those agencies have a legitimate need to the information, and have confidentiality and data protection policies in place which provide equivalent protection of the information.

Inn Churches will ensure that services users know how and why we collect, process and store information about them, and how it could be shared, as well as their rights under data protection law, through a publicly available privacy notice.

Breaking confidentiality

Confidentiality should only be broken (without the data subject's consent) in exceptional circumstances, where due to the urgency and seriousness of the situation it is not possible to seek consent (for example preventing the person causing serious harm to themselves or others), or where the law requires it (for example a request from the police or courts) and consent is not given. Approval to break confidence in these circumstances must be obtained from the Project Coordinator / CEO or Chair of Trustees, and the Trustees must be informed.

Where there are concerns about the welfare or safety or a child or vulnerable adult, the procedures in the safeguarding policy should be followed. Note that this may mean sharing confidential information about individuals without the need to inform them (or their parents / guardians), if doing so would have the potential to cause further harm or jeopardise any subsequent legal investigation. This is permitted under data protection law, and indeed there is a legal (and moral) obligation to do so. Any information shared should still be shared following the principles in this policy, and be the minimum information necessary for the purpose.

Other breaches of confidentiality (whether deliberate or accidental) are a serious matter which will be dealt with by the Trustees and may results in dismissal or prosecution. For staff this may mean following the disciplinary procedures. For other individuals this many mean summarily ending their association with Inn Churches.

Reporting a breach

All personal data breaches must be recorded, and reported to the Trustees, either at their next meeting, or immediately in the case of a reportable breach.

When a breach occurs, the Data Protection Lead will decide whether or not it needs reporting to the ICO, police or other agency. Failing to report a breach can result in a significant fine.

If the Data Protection Lead decides that reporting is necessary, the breach must be reported to the Information Commissioner's Office on 0303 123 1113, and any other appropriate body within 72 hours. If the breach may adversely affect any individual, they must also be informed of it without undue delay.

The Trustees will also need to cooperate with any ensuing investigation or prosecution.

Data protection

Data protection laws outline how organisations must collect, process and store personal data relating to living identifiable individuals. This may include (but is not limited to) name, address, email, postcode, CCTV image, photograph and special category data (racial or ethnic origin, political opinion, religious beliefs, mental or physical health, sexual health, trade union membership and criminal convictions).

Inn Churches is committed to processing data in accordance with its responsibilities under data protection laws.

We will ensure that all personal data 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;

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 and up-to-date technical or organisational measures.

The current data protection laws this policy enacts are the General Data Protection Regulations (EU) 2016/679 (GDPR) and the UK Data Protection Act 2018 (DPA2018) as amended by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019, and the Privacy and Electronic Communications Regulations (PECR).

This policy applies to all data processed by Inn Churches, whether on Inn Churches premises or accessed from home or mobile working, on any device and in any format.

Training, roles and review

Inn Churches will ensure that all staff are aware of best practice in data protection, and know where to find support and guidance for data protection issues. Adequate and role-specific training will be provided to all staff and volunteers roles who process personal data, to ensure that workers understand their responsibilities when processing such data.

The Data Protection Lead is Juli Thompson (CEO).

This policy will be reviewed annually.

Individual rights

Inn Churches will ensure that data subjects' rights are upheld, and that they are aware of these rights and how to exercise them, to ensure that they retain control over their data.

These rights are the:

- Right to be informed
  We will inform individuals of how and why we are processing their data, and these rights, in an understandable and easily accessible form.
- Right to access
  We will ensure that individuals know that they are entitled to obtain confirmation that their data is being processed, and copies of that data. Requests for access will be processed as soon as possible, and within 28 days.
- Right to rectification
  We will ensure that we correct inaccurate data when it is brought to our attention. Requests for rectification will be processed as soon as possible, and within 14 days.
- Right to erasure ("the right to be forgotten")
  We will ensure that individuals know that they are entitled to have their data erased if it is no longer necessary for the purpose for which it was originally collected, or if it is stored based on consent and they withdraw that consent. Requests for erasure will be processed as soon as possible, and within 28 days.
- Right to restrict processing
  We will ensure that individuals are aware that they are entitled to restrict the processing of their data, upon request. Requests to restrict processing will be processed as soon as possible, and within 14 days.
- Right to data portability
  We will ensure that individuals can transfer their data to a similar organisation, in the format required, upon request. Requests for data portability will be processed as soon as possible, and within 28 days.
- Right to object
  We will ensure that individuals are aware that they can object to the processing of their personal data in certain circumstances, and comply with such objections, except where the grounds for processing data can be demonstrated to override the interests, rights and freedoms of the individual, or the processing is for the establishment, exercise or defence of a legal claim.

Data processing and retention

Access to personal data shall be limited to workers who need access. Appropriate security should be in place to avoid unauthorised sharing of information.

Where consent is relied upon as a lawful basis for processing data, evidence of opt-in consent will be kept with the personal data. Where communications are sent to individuals based on their consent, the option for the individual to revoke their consent should be clearly available in each communication and systems will be in place to ensure such revocation is reflected accurately.

Where third parties are engaged who will process data on behalf of Inn Churches, we will ensure that they have appropriate technical security measures in place, and that any sub-processors are agreed.

When personal data is deleted, it will be done safely such that the data is irrecoverable.

In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, the Charity shall promptly assess the risk to people's rights and freedoms as detailed in the breach processes above.

Details of how Inn Churches processes data, and the third party data processors involved, are contained in appendix 1.

Data sharing

Where data is shared with other agencies, appropriate security measures will be in place to ensure that data cannot be intercepted or misplaced.

Where data is shared regularly, a contract or data sharing agreement will be in place to outline the data being shared and agreed purpose.

Any data sharing will be detailed in the relevant privacy notice.

Appendix 1: Data Processing and Processors

Inn Churches process data in the following ways:

Process	Third parties	Lawful bases	Archive policy
Inn Churches engages the services of Ben Clymo t/a Bromeliad Services who is a third party data processor on all of the processes above.			
Inn Churches' websites are hosted by VTS Hosting, and therefore data submitted via our website is processed by VTS Hosting. The website referral forms on our website feed data into a Google Sheets or Microsoft Excel file and therefore Google and Microsoft are third party data processors of any referrals.			
Inn Churches' emails and documents are hosted on Microsoft 365 and therefore Microsoft is a third party data processor of any information submitted by email or stored in our cloud storage.			
For FoodSavers membership data, the relevant FoodSavers outlet is a third party data processor, and the relevant Credit Union is a third party data controller.			
Website form contact		Consent, legitimate interest	Messages retained for one year on website server, then deleted.
Names and email addresses for email mailing list via website signup, or paper signup sheets for events	MailChimp Sender.net	Consent	Details removed when unsubscribed. Signup sheets kept as proof of consent, entries blacked out if requested.

Personal details of Winter Shelter guests via an online referral form	Google	Consent, legitimate interest, vital interest	Digital records retained for three years after referral date, then anonymised. Paper records retained for three years after referral date, then destroyed.
Personal details of volunteers via an online application form	Microsoft	Consent, contract	Original website, paper application form, and/or digital copy of paper application form retained for six months after application (if not appointed), or one year following volunteering end (if appointed), then destroyed.
Personal details of FoodSavers customers	Microsoft FoodSavers outlet For savers with a Credit Union, that Credit Union	Consent, contract, legitimate interest	Paper records are digitised and then destroyed. Records of ID required to open a Credit Union account are transferred to the Credit Union, and retained by us until the account is opened and then destroyed. Credit Unions keep those records transferred to them in line with their own policies. Digital records retained for three years after last visit, and then anonymised. Duplicate or additional records kept by FoodSavers outlets in line with their own policies.
Personal details of users of the Acts435 service	Acts435 Microsoft	Consent, legitimate interest	Digital records retained for three years after referral date, then anonymised. Paper records retained for three years after referral date, then destroyed. Digital records kept by Acts 435 in line with their own policies.

Personal details of users of the Starter Pack service	Microsoft	Consent, legitimate interest	Digital records retained for three years after referral date, then anonymised. Paper records retained for three years after referral date, then destroyed.
Personal details of users of the Warm Homes Healthy People service	Groundwork / Salesforce Microsoft	Consent, legitimate interest	Digital records retained for three years after referral date, then anonymised. Paper records retained for three years after referral date, then destroyed. Digital records kept by Groundwork (stored on Salesforce) in line with their own policies.
Names, addresses and payment details of people making payments or donations (including Gift Aid declarations) via our websites, by phone or in person	PayPal KindLink	Consent, contract, legal obligation (Gift Aid)	Gift Aid declarations retained for six years after latest donation being made, then destroyed. Donor and donation details or donations made through our websites stored by Kindlink in line with their policies. Digital or paper records, or digital copies of paper records, retained for six years after the financial year end of the financial year the donation made in, then destroyed.
Payroll and health & safety information for Inn Churches staff	Torevell Dent	Consent, contract legal obligation, legitimate interest	Retained for six years after ceasing employment, then destroyed.