TOWN HALL \ Hebden Bridge

Data Protection Policy
Version 1

Contents

1. Aims

Hebden Bridge Community Association Ltd at the Town Hall aims to ensure that all personal data collected about staff, volunteers, trustees, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation and the provisions of the Data Protection Act 2018 (DPA 2018).

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

This policy is also applicable to our trading subsidiary The Town Hall Café Ltd (registered company number 09981542) a wholly owned subsidiary of Hebden Bridge Community Association which donates any surplus to Hebden Bridge Community Association.

2. Legislation and guidance

This policy meets the requirements of the GDPR and the provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests.

It also reflects the ICO's code of practice for the use of surveillance cameras and personal information.

3. Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, individual. This may include the individual's: • Name (including initials) • Postal Address • Telephone Number • Email address • Bank details (if you are donating to us). It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental • Sex life or sexual orientation **We do not collect ANY of this data about individuals.**
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.

Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

4. The data controller

Hebden Bridge Community Association processes personal data relating to staff, volunteers, trustees, visitors and other individuals, and therefore is a **data controller**. The Trustees of Hebden Bridge Community Association are formally the **data controllers.**

Hebden Bridge Community Association is registered as a **data controller** with the ICO and will renew this registration annually or as otherwise legally required.

5. Roles and responsibilities

This policy applies to **all staff** employed by Hebden Bridge Community Association, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

5.1 The Trustee Board

The Trustees of Hebden Bridge Community Association have overall responsibility for ensuring that the organisation complies with all relevant data protection obligations.

5.2 Data Protection Officer

The Data Protection Officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

The DPO will provide an annual report of activities directly to the Trustees and, where relevant, report to the Trustees advice and recommendations on our data protection issues.

The DPO is also the first point of contact for individuals whose data we process, and for the ICO.

Full details of the DPO's responsibilities are set out in their job description.

Our DPO is Graham Mynott (the Executive Director) and is contactable via The Town Hall, George Street, Hebden Bridge, West Yorkshire, HX7 7BY. 01422 417 300

5.3 The Executive Director

The DPO (Executive Director) acts as the representative of the data controllers on a day-to-day basis.

5.4 All staff

Staff of Hebden Bridge Community Association are responsible for:

- Collecting, storing and processing personal data in accordance with this policy
- Informing Hebden Bridge Community Association of any changes to their personal data, such as a change of address
- Contacting the DPO in the following circumstances:
    - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
    - If they have any concerns that this policy is not being followed
    - If they are unsure whether or not they have a lawful basis to use personal data in a particular way
    - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area

- If there has been a data breach
- Whenever they are engaging in a new activity that may affect the privacy rights of individuals
- If they need help with any contracts or sharing personal data with third parties

6. Data protection principles

The GDPR is based on data protection principles that we must comply with.

The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

This policy and our associated Privacy Policy set out how we comply with these principles.

7. Collecting personal data

7.1 Lawfulness, fairness and transparency

We can only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that Hebden Bridge Community Association can **fulfil a contract** with the individual, or the individual has asked the Town Hall to take specific steps before entering into a contract
- The data needs to be processed so that Hebden Bridge Community Association can **comply with a legal obligation**
- The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone's life
- The data needs to be processed so that Hebden Bridge Community Association, as a members charity, can perform a task **in the public interest,** and carry out its official functions
- The data needs to be processed for the **legitimate interests** of Hebden Bridge Community Association or a third party (provided the individual's rights and freedoms are not overridden)
- The individual has freely given clear **consent**

We do not collect any special categories of personal data.

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law. This is set out in our Privacy Policy.

7.2 Limitation, minimisation and accuracy

We only collect personal data for specified, explicit and legitimate reasons. We explain these reasons to the individuals when we first collect their data. This is set out in our Privacy Policy.

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs.

When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with Hebden Bridge Community Association Document Retention Policy.

8. Sharing personal data

As set out in our Privacy Policy we do not sell, trade, rent personal data we hold to any third parties.

This is an extract from our Privacy Policy:

In the future we may employ carefully selected third parties to provide services on our behalf, including undertake fundraising, sending mailings, marketing communications and for research purposes.

We will only use a third party where it is more cost effective for the charity to do so or we are unable to facilitate this activity internally. Please be reassured that we would ensure any company delivering services on our behalf are equally vigilant about safeguarding your data and any such activity will be subject to data processing agreements.

We only disclose information to third parties or individuals when obliged to by law, for purposes of national security, taxation and criminal investigations.

9. Subject access requests and other rights of individuals

9.1 Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that Hebden Bridge Community Association holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

Subject access requests must be submitted in writing, either by letter or email to the DPO. They should include:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested

If other staff receive a subject access request they must immediately forward it to the DPO.

9.2 Responding to subject access requests

When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request
- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of another individual
- Would reveal that an individual is at risk of abuse, where the disclosure of that information would not be in the person's best interests

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs.

A request will be deemed to be unfounded or excessive if it is repetitive, or asks for further copies of the same information.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

9.3 Other data protection rights of the individual

These are also set out in our Privacy Policy.

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the DPO. If other staff receive such a request, they must immediately forward it to the DPO.

10. CCTV

Please see our Privacy Policy which contains a specific CCTV section along with our separate CCTV Policy.

11. Photographs and videos

As part of Hebden Bridge Community Association's marketing activities, we may take photographs and videos recording images of individuals within our premises.

Uses may include:

- Within the Town Hall on notice boards and in our newsletters, etc.
- Outside of the Town Hall by external agencies
- Online on our website or social media pages

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

When using photographs and videos in this way we will not accompany them with any other personal information about the individual, to ensure they cannot be identified.

12. Data protection by design and default

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)
- Completing privacy impact assessments where our processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
    - For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

13. Data security and storage of records

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use
- Papers containing confidential personal data must not be pinned to notice/display boards, or left anywhere else where there is general access
- Not allowing personal information to be taken off site
- Password protection on our computers, laptops and other electronic devices. Staff are reminded to change their passwords at regular intervals through the Razorblue supported computers
- Staff who store personal information on their personal devices are expected to follow the same security procedures as for Hebden Bridge Community Association-owned equipment
- We do not share personal data with third parties

14. Disposal of records

Personal data that is no longer needed – in line with our Document Retention Policy - will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on our behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

15. Personal data breaches

The Town Hall will make all reasonable endeavours to ensure that there are no personal data breaches.

In the unlikely event of a suspected data breach, we will follow the procedure set out in appendix 1.

When appropriate, we will report the data breach to the ICO within 72 hours.

16. Training

All staff and trustees are provided with data protection training as part of their induction process.

Data protection will also form part of continuing professional development, where changes to legislation, guidance or our processes make it necessary.

17. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed and updated if necessary when there are legislative or GDPR guidance amendments. Otherwise, or from then on, this policy will be reviewed **every 2 years** and shared with the full trustee board.

18. Links with other policies

This data protection policy is linked to our:

- Privacy Policy
- CCTV Policy
- Document Retention Policy

VERSION CONTROL			
Date	**Version Number**	**Originator**	**Amends**
May 2018	DRAFT	Amanda Ward	
April 2019	V1	Graham Mynott	Review & Updated

Appendix 1: Personal data breach procedure

This procedure is based on ICO guidance an personal data breaches.

- On finding or causing a breach, or potential breach, the staff member or other data processor must immediately notify the DPO
- The DPO will investigate the report, and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
    - Lost
    - Stolen
    - Destroyed
    - Altered
    - Disclosed or made available where it should not have been
    - Made available to unauthorised people
- The DPO will alert the Chair of Trustees
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or other data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen
- The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
    - Loss of control over their data
    - Discrimination
    - Identify theft or fraud
    - Financial loss
    - Unauthorised reversal of pseudonymisation (for example, key-coding)
    - Damage to reputation
    - Loss of confidentiality
    - Any other significant economic or social disadvantage to the individual(s) concerned

  If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.
- The DPO will document the decision (either way); in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on the Association's computer system
- Where the ICO must be notified, the DPO will do this via the "report a breach" page of the ICO website within 72 hours. As required, the DPO will set out:
    - A description of the nature of the personal data breach including, where possible:
        - The categories and approximate number of individuals concerned
        - The categories and approximate number of personal data records concerned
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned

- If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible
- The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned
- The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
    - Facts and cause
    - Effects
    - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

  Records of all breaches will be stored on the Town Hall's computer system
- The DPO and Chair of Trustees will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible

Actions to minimise the impact of data breaches

We will take the actions set out below to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

Sensitive information being disclosed via email

- *If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error*
- *Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error*
- *In any cases where the recall is unsuccessful, the DPO will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way*
- *The DPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request*
- *The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted*