Data Protection & Confidentiality Policy

January 2022

Last Reviewed: January 2022

Purpose

The security and management of data is important to ensure that Holywood Shared Town (HST) can function effectively and to ensure compliance with legislation and statutory guidelines.

It is essential that the data of trustees, members or other people is protected through the lawful and appropriate use and handling of their personal information to ensure their privacy.

The use of all personal data by HST is governed by:

- The General Data Protection Regulation (GDPR)
- The UK Data Protection Act 2018 (DPA)
- The Privacy and Electronic Communications Regulations (PECR)

Every person who handles data on behalf of HST has a responsibility to adhere to the Data Protection Principles outlined in the GDPR, and to this Data Protection Policy.

Scope

- This policy applies to anyone who handles or processes personal data on behalf of Holywood Shared Town (voluntary or employed) which may include the board of trustees, any paid staff, volunteers, sessional workers etc.

Data Protection Overview

There are six data protection principles defined in Article 5 of the GDPR. These require that all personal data be:

- processed in a lawful, fair and transparent manner.
- collected only for specific, explicit and limited purposes ('purpose limitation').
- adequate, relevant and not excessive ('data minimisation').
- accurate and kept up-to-date where necessary.
- kept for no longer than necessary ('retention').
- handled with appropriate security and confidentiality.

HST is committed to upholding the data protection principles. All personal data under our control must be processed in accordance with these principles.

Lawful processing

All processing of personal data must meet one of the six lawful bases defined in Article 6(2) of the GDPR:

- Where there is the consent of the data subject
- Where it is in HST's legitimate interests and this is not overridden by the rights and freedoms of the data subject
- Where necessary to meet a legal obligation
- Where necessary to fulfil a contract, or pre-contractual obligations
- Where HST is protecting someone's vital interests
- Where HST is fulfilling a public task, or acting under official authority.

Any special category data (sensitive types of personal data as defined in Article 9(1) of the GDPR) must further be processed only in the line with one of the conditions specified in Article 9(2).

Rights of data subjects

Under data protection laws, data subjects have certain rights:

1. Right to be informed - the right to be told how their personal data is used in clear and transparent language.
2. Right of access - the right to know and have access to the personal data held about them.
3. Right to data portability - the right to receive their data in a common and machine-readable electronic format.
4. Right to be forgotten - the right to have their personal data erased.
5. Right to rectification - the right to have their personal data corrected where it is inaccurate or incomplete.
6. Right to object - the right to complain and to object to processing.
7. Right to purpose limitation - the right to limit the extent of the processing of their personal data.
8. Rights related to automated decision-making and profiling - the right not to be subject to decisions without human involvement.

Policy

Holywood Shared Town recognises that colleagues (employees, volunteers, trustees, secondees and students) gain information about individuals and organisations during the course of their work or activities. In most cases such information will not be stated as confidential, and colleagues must exercise common sense and discretion in identifying whether this information should be communicated to others. Information given in confidence must not be disclosed without consent unless there is a justifiable reason e.g. a requirement of law or there is an overriding public interest to do so.

Confidential information includes anything that contains the means to identify a person, e.g. name, address, post code, date of birth, National Insurance Number, passport and bank details. It includes information about sexual life, beliefs, commission or alleged commission of offences and other sensitive

personal information as defined by the Data Protection Act. It also includes information about organisations such as confidential business plans, financial information, contracts, trade secrets and procurement information

HST generally processes data of Trustees and members in line with its activities. This data will not be used for any purpose other than the purpose for which it was stipulated when requesting the data i.e. a trustee's name, address and other personal information collected when they join HST is used for the purpose of reporting to the NI Charity Commission and Companies House.

Why information is held

- Most information held by Holywood Shared Town relates to individuals, activity members, service users, voluntary and community organisations, self-help groups, volunteers, students, employees, trustees or services which support or fund them.

- Information is stored to enable Holywood Shared Town colleagues to understand the history and activities of individuals or organisations in order to deliver the most appropriate services.
- Holywood Shared Town has a role in putting people in touch with voluntary and community organisations and keeps contact details which are passed on to any enquirer, except where the group or organisation expressly requests that the details remain confidential.
- Information about students is given to the training organisation and the college, but to no one else.
- Information about protected equality characteristics of users is kept for the purposes of monitoring our equal opportunities policy and also for reporting back to funders.

Where processing is based on consent, the data subject has the option to easily withdraw their consent.

HST will uphold individuals' rights under data protection laws and allow them to exercise their rights over the personal data held about them by HST. Most rights are not absolute, and the individual will be able to exercise them depending on the circumstances, and exemptions may apply in some cases. Any request in respect of these rights should preferably be made in writing to the Chair.

Where a request is made to HST regarding their data, HST will:

- Not charge for facilitating a request, unless it is 'manifestly unfounded or excessive', in which case administrative costs can be recovered.
- Reserve the right to refuse requests that are 'manifestly unfounded or excessive'.
- Take reasonable measures to require individuals to prove their identity where it is not obvious that they are the data subject.
- Respond to any request within one month from the date of request or being able to identify the person, unless it is particularly complex (in which case no longer than 90 days).

Data minimisation and control

HST, in processing personal data, will:

- Keep the personal data collected, use and share to the minimum amount required to be adequate for its purpose
- Where there is no legal obligation to retain some personal data, regularly consider whether there is a lawful organisational need to hold it
- Retain personal data only for as long as it is necessary to meet its purpose and where data is no longer required to be held, destroy this data

- In the case of sharing personal data with any third party, disclose only the data that is necessary to fulfil the purpose of sharing
- Consider anonymisation and pseudonymisation of personal data stored or transferred where possible.

Organisational measures

In so far as is possible, HST will implement organisational measures to protect the data of all subjects which may include:

- Devices having hardware encryption set up by default where possible, including laptops, mobile devices and removable media.
- Sharing this policy with all persons who handle or process personal data on behalf of HST.
- Requiring any contractor, temporary worker, consultant, or anyone else working on behalf of HST who fails in their obligations under this Policy, to indemnify HST against any cost, liabilities, damages, loss, claims or proceedings that may arise from that failure.

Procedure

Confidentiality

All persons who may be party to personal information should abide by the following:

- Colleagues should seek advice from the Chair about confidentiality and sharing information as necessary.
- Colleagues will avoid exchanging personal information or comments about individuals with whom they have a professional relationship.
- Talking about the private life of a colleague is to be avoided at all times, unless the colleague in question has instigated the conversation.
- Colleagues will avoid discussing confidential information about organisations or individuals in social settings.
- Colleagues will not disclose to anyone, other than a designated person responsible for their supervision, any information considered sensitive, personal, financial or private without the knowledge or consent of the individual, or an officer, in the case of an organisation.
- Where there is a statutory duty on Holywood Shared Town to disclose information, the person or people involved will usually be informed that disclosure has or will be made unless this would put at risk the safety of any individual or jeopardise a potential criminal investigation.
- Details about disclosure of information and who has been informed will always be kept on record and stored securely with restricted access.

Access to information

Information is confidential to Holywood Shared Town as an organisation and may be passed to colleagues, line managers or trustees on a need to know basis to ensure the best quality service for users.

Where information is sensitive, i.e. it involves disputes or legal issues, it will be confidential to the person dealing with the case and supervisor. Such information should be clearly labelled ‘Confidential’

and should state the names of the colleagues entitled to access the information and the name of any individual or group who may request access to the information. Colleagues will not withhold information from their supervisor unless it is purely personal.

When photocopying or working on confidential documents, colleagues should ensure people passing do not see them. This also applies to information on computer screens.

Processing/handling data

All persons who handle or process personal data on behalf of HST must comply with these procedures for processing or transmitting personal data:

- Always treat people's personal information with integrity and confidentiality.
- Where personal data exists as hard copy, it should be stored in a locked box, drawer or cabinet, and not left where someone who does not have authority to access it. Files or filing cabinet drawers bearing confidential information should be labelled 'confidential'.
- The loss or theft of any device with personal data that has been collected on behalf of HST stored upon it should be reported as soon as possible to the Chair or Board Secretary.
- Take all reasonable care to email the intended recipient (especially where email address autocomplete is turned on), use 'bcc' field for emailing several people where using 'to' or 'cc' is not needed.
- Ensure any device used for personal data has a firewall and the data is password protected.
- In an emergency situation, the Chair may authorise access to files by other people.

Reporting breaches

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

All persons who handle/process personal data on behalf of HST should be vigilant and able to identify a suspected personal data breach.

A breach could include:

- loss or theft of devices or data, including information stored on USB drives or on paper
- hacking or other forms of unauthorised access to a device, email account, or the network
- disclosing personal data to the wrong person, through wrongly addressed emails, or bulk emails that inappropriately reveal all recipients email addresses
- alteration or destruction of personal data without permission
- Where a personal data breach is suspected or discovered, this should be reported to the Chair as soon as possible
- Where there is a likely risk to individuals' rights and freedoms, the breach will be reported by the Chair to the ICO within 72 hours of HST becoming being aware of the breach and inform those individuals without undue delay
- HST will keep a record of all personal data breaches reported and follow up with appropriate measures and improvements to reduce the risk of reoccurrence.

Duty to disclose

In exceptional circumstances HST may have a legal duty to disclose confidential information, for example:

Child and adult safeguarding concerns/disclosures may be reported to the relevant statutory services

Drug trafficking, money laundering or acts of terrorism or other criminal activity disclosed to the PSNI.

Where it is appropriate and possible to do so, an individual will be informed of any disclosures of their confidential information unless this would put at risk the safety of any individual or jeopardise a potential criminal investigation. Details about disclosure of information and who has been informed will be kept on record and stored securely with restricted access

Criminal Records Checking – Disclosures of Criminal Convictions

Holywood Shared Town complies fully with accepted codes of practice (Access NI) regarding the correct handling, use, storage, retention and disposal of Disclosures and Disclosure information.

Access NI Disclosure Certificates will not be retained by HST except where such a disclosure has an impact on a recruitment decision. Where this is the case, any record will be kept securely and access to the information limited.

Signed: John Woods

Chair/Trustee Holywood Shared Town

Date: 4 January 2022

Review date: January 2025