Stockbridge Town Hall CIO
Data Protection Policy
Approved by email vote following meeting of 15 April 2019

Note: there is a separate policy on retention and use of CCTV images.

Stockbridge Town Hall Charitable Incorporated Organisation and its wholly owned subsidiary Stockbridge Town Hall Trading Company Limited needs to collect and use certain types of information about individuals and organisations, such as Hall Users, Trustees, Donors, Friends, Contractors and Employees. This information must be collected and dealt with appropriately, whether it is collected or stored on paper, computers or by any other means, in accordance with the General Data Protection Regulations [GDPR] that came into force on the 25th of May 2018.

Note The General Data Protection Regulations apply only to 'Personal Information' defined as information relating to an identified or identifiable natural person but this policy covers data collected and processed about individuals and organisations. This is for ease of operation and avoids the need to differentiate at the point of data collection

Privacy Notice
At the point of data collection a 'Privacy Notice' (see Appendix A) stating what will happen to the data collected will be issued to the Individual or Organisation submitting the data [termed Data Subjects].

Data Protection Principles
All data collected shall be:

1. Processed fairly, lawfully and in a transparent manner
2. Used only for the lawful purposes of managing the hall
3. Adequate, relevant and not excessive in relation to those purposes
4. Accurate and up-to-date
5. Kept for ten years and then securely destroyed
6. Processed in accordance with the rights of the Data Subject under the above Regulations
7. Kept secure, confidential and not shared with any third party ,other than the organisation providing a back-up service for the computer system, unless legally required

Data Register
A register will be maintained detailing

1. What data is held
2. Why the data is held
3. The source of that data
4. Where the data is located
5. Who has access to that data
6. What type of consent is relevant
7. What level of security is applicable

8. With whom the data is shared
9. The retention period for that data
10. The process of disposing of that data

Rights of Data Subjects

Individuals or Organisations submitting data for processing have the right;

1. To be informed regarding the data held about them, where it is held, the purpose for which it is held and how it is processed
2. To have access to the data held
3. To request rectification to the data held

Data Subjects wishing to exercise these rights must put their request [termed a Subject Access Request] in writing to the Data Protection Officer and must provide proof of their identity.

Any action required to deliver these rights must be taken within 30 days and the Data Subject informed.

Data Subjects not satisfied by the response have the right to refer the matter to The Information Commissioner's Office.

Risk

Data Processing must be integrated into activities and processes as part of risk management planning. Where there is a high risk that cannot be adequately addressed then The Information Commissioner's Office must be informed

Data Protection Officer

A Trustee is appointed as the Data Protection Officer (DPO), see annual Business Plan. The DPO and is responsible for

1. Ensuring compliance with the Data Protection Regulations
2. Dealing with Subject Access Requests
3. Maintaining the Data Register
4. Ensuring that everyone processing data follows good data protection practices
5. Dealing with data breaches

The DPO is registered with the Information Commissioner's Office – reference number ZA345130.

The current DPO is Mark Frank (mark.t.frank@gmail.com).

Policy Review

This policy will be reviewed annually and updated where necessary. A copy of this policy will be available for public inspection on the Town Hall web site.