TULLYNESSLE & FORBES HALL

TULLYNESSLE & FORBES COMMUNITY & HALL ASSOCIATION
GDPR PRIVACY POLICY

1.0 INTRODUCTION

In the course of normal business, Tullynessle & Forbes Community & Hall Association (the Hall) is required to gather and use certain information, known as personal data, about individuals.

Such individuals, called Data Subjects, include, but are not limited to:

- Clients
- Staff
- Volunteers
- Contractors
- Suppliers
- Other parties that the organisation has a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled and stored (processed) to meet our data protection standards AND to comply with the relevant legislation.

2.0 PURPOSE

This data protection policy ensures that the Hall:

- Complies with the relevant data protection legislation and follows good practice
- Protects the rights of all relevant data subjects
- Is open and transparent about how it processes personal data
- Protects itself from the risks of a data breach

3.0 SCOPE

The scope of this procedure applies to the following:

- All working locations (Home, Hall, Home Office, Office)
- All staff and volunteers
- All sessional workers/contractors operating on behalf of the Hall

It applies to all data that the Hall holds relating to identifiable individuals including, but not limited to:

- Name
- Postal address
- Email address
- Date of birth
- Telephone numbers
- Unique reference numbers or identifiers
- Bank Details
- Employment History
- And any other identifiable information relating to individuals, including special categories (sensitive)

4.0 DATA PROTECTION LEGISLATION

The following key legislation and guidance informs the Hall regarding the development of our procedures and controls:

- General Data Protection Regulation (GDPR)
- Data Protection Act 2018
- Privacy and Electronic Communications Regulation 2003 (PECR)

These legal requirements govern how we will collect, handle and store personal data. They apply regardless of whether the data is stored electronically, on paper or on other materials. To comply with the law, the following EIGHT principles must be applied and evidenced. Personal data must be:

1. Processed fairly, lawfully and transparently
2. Be obtained only for specific and lawful purposes
3. Be adequate, relevant and not excessive
4. Be accurate and kept up-to-date
5. Not be held for longer than necessary
6. Processed in accordance with the rights of the data subjects (individuals)
7. Be protected in appropriate ways to prevent accidental or intentional loss, modification, destruction
8. Not be transferred outside of the European Economic Area (EEA) without adequate protection

5.0 RISKS

This policy helps to protect both the Hall and its data subjects from very real data security risks including:

- ✓ **Breaches of confidentiality**, e.g information being disclosed inappropriately
- ✓ **Reputational damage**, e.g. complaints, legal proceedings, negative media, etc
- ✓ **Financial costs**, e.g. compensation, fines, etc.

6.0 RESPONSIBILITIES

Everyone who handles/processes personal data on behalf of the Hall must ensure that it is done so in line with this policy and all other related procedures.

7.0 GUIDELINES

- The only people who can access the personal data, covered by this Policy, are those who are required to use it for their legitimate work and who are authorised to do so.
- Data must not be shared informally. Personal data must be treated with the utmost confidence and security at all times.
- The Hall will provide training to all employees, partners, contractors, etc to ensure that they are fully aware and understand their responsibilities regarding data protection and privacy
- For system access, strong passwords must be used and never shared
- Personal data should never be disclosed to unauthorised persons, either within the business or externally.
- Data should be regularly reviewed (by authorised personnel) and updated according. If there is no longer a legal basis or legitimate purpose for retaining the personal data, it must be securely deleted/destroyed.
- Where consent is the legal basis for processing information, regular reviews must be undertaken to ensure that the individual still consents to sharing their personal data.
- In certain circumstances, individuals reserve the right to withdraw their consent to processing their personal data
- Individuals may request information regarding the personal data processed by the Hall. This is called a Subject Access Request (SAR) and must be processed in line with standard SAR Procedures.
- Individuals may raise a query or complaint at any time. The contact details for communications relating to data protection are at the end of this document.

8.0 LEGAL BASIS

Under the new legislation, a lawful justification, called a Legal Basis, must be identified and evidenced before personal data can be processed. There are SIX Legal Bases, as detailed below:

1. CONSENT
2. CONTRACT
3. LEGAL OBLIGATION
4. PUBLIC INTEREST
5. VITAL INTEREST
6. LEGITIMATE INTEREST

9.0 CONSENT

The new legislation has provided a more detailed definition of Consent. Consent cannot be assumed or implied and must be:

- ✓ Freely given
- ✓ Specific
- ✓ Informed
- ✓ Unambiguous
- ✓ Given by clear statement or affirmative action

Prior to obtaining consent, individuals will be provided with access to the relevant privacy notice (also sometimes referred to as a Privacy Policy or a Fair Processing Notice). See Section 16.0.

Where data processing requires consent, the Hall will conduct regular consent audits and contact the relevant individuals to establish that consent is still current and given as above.

10.0 SPECIAL CATEGORIES (only if applicable)

This relates to the processing of sensitive data that must be treated with a high degree of care. Special categories of data includes racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data and data concerning health or reveal their sex life or sexual orientation.

Processing this data is prohibited unless EXPLICIT consent is obtained from the individual or, in certain circumstances, where processing is necessary. Some examples of when special categories personal data can be processed without explicit consent include (but are not limited to):

- in the field of employment, social security and social protection law,
- the provision of occupation health services,
- for legal or public health reasons

For further information regarding special categories personal data, please contact the Company Data Protection Representative.

11.0 PROCESSING ACTIVITIES & CONTROLS

To ensure adequate controls and rules exist to manage the processing of personal data that exists across the organisation, the Summary Record of Processing Activities (ROPA) documents the various processing activities that occur.

The Hall ROPA details the type of personal data processed, the purpose, legal basis and storage/retention rules below.

Questions regarding processing activities, including storage, should be directed to the Data Protection Representative.

Hall ROPA:

When data is stored in a physical format (paper, etc), it will be kept in a secure location where unauthorised persons cannot get access. These guidelines also apply to data that is stored electronically, but that has been printed out.

- Paper files, when not being processed, will be stored in a locked drawer/cabinet.
- Employees shall ensure that paper/prints that contain personal data shall not be left unattended, eg. on a printer or left on a desk, where non-authorised persons can see them.
- When no longer required, paper/prints shall be shredded and disposed of securely

When data is stored electronically, it must be protected from unauthorised access, accidental disclosure/loss, accidental deletion or malicious hacking attempts:

- Data must be protected with strong passwords, that are changed regularly and never shared
- Data stored on removable media (DVD, CD, USB, etc) must be stored securely and locked away when not in use
- Data should be backed up regularly.
- All services and computers containing data should be protected by approved security software and a firewall, as appropriate.
- Financial data will be retained for a period of 7 years according to HMRC recommendations.

12.0 DATA MINIMISATION

Data will be held in as few places as necessary and only retained in line with the data storage requirements as documented in the Summary Record of Processing Activities (ROPA) above.

13.0 DATA SUBJECTS RIGHTS

In line with the legislation, individuals have more rights to ensure the protection of their privacy and the security of their data. This section details their rights and how (Company Name) will respond to them.

13.1 Subject Access Requests (SAR)

All individuals are entitled to:

- ✓ Ask what information the Hall holds about them and why
- ✓ Ask how to gain access to it
- ✓ Be informed about how we keep it up to date
- ✓ Be informed about how the Hall is meeting its data protection and privacy obligations

If an individual requests to receive this information, it is called a Subject Access Request (SAR). The Hall will always verify the identity of the requester and no information will be sent out until that has been undertaken. Approved identity documents will be one that is photographic (national ID card, drivers licence or passport) and one current utility bill.

SARS may be requested in any medium (verbally, email, physical letter) and the Hall has a legal obligation to provide all information processed within 1 month of receiving the request. Ordinarily, there is no charge for this, however, if the SAR is significant in terms of size/complexity, the Hall does reserve the right to apply an administration fee.

Please note, however, there may be certain circumstances where it is not possible to provide all SAR's information (in line with the Law). If this is the case, the person will be fully informed.

13.2 Right to Rectification

In the event that it is discovered that the Hall is holding inaccurate or out of date personal data relating to an individual, that individual has the right to request that the data is amended/rectified as quickly as possible.

13.3 Right to Erasure

Whilst an individual does have the right to request erasure of their data (also called the Right to be Forgotten) it is not an absolute right, as there are only certain instances where their request can be accepted. The right can be fulfilled in the following circumstances:

- The personal data is no longer required by the Hall in relation to the purposes that originally applied
- The individual has withdrawn their consent and there is no other legal basis for processing
- The individual objects to the Hall processing their data and there are no overriding legitimate grounds for continuing to process.
- The personal data has been unlawfully processed
- A legal obligation (e.g. a court order) requires the data to be erased
- The data relates to a child and there is no parental consent

If the right to erasure is accepted the Hall must take reasonable steps to destroy all data, including any that has been made public (e.g. photographs, video clips, etc) and any data that has been forwarded/shared with other agreed 3rd parties, including processors.

The right to erasure may not be accepted for legal or public health reasons.

13.4 Right to Restriction of Processing

An individual has the right to restrict processing in the following instances:

- The accuracy of the data is contested and time is required to verify
- The processing of the data is considered unlawful but erasure isn't an option
- The Hall no longer needs the data but it may be required to support a legal claim
- The individual has objected to processing and verification is required to establish legitimate grounds

13.5 Right to Data Portability

The individual has the right to request all their personal data held by the Hall, receive it in a machine-readable format and request that it be transferred to another Data Controller. This is applicable when the data is processed by automated means only.

14.0 DATA BREACHES

The Hall have a responsibility for ensuring that all personal data is securely managed and protected to prevent unauthorised or accidental access, disclosure or loss that would pose a risk to an individual. In the event of perceived data breach, please contact the Data Protection Representative referenced at the end of this document.

15.0 DISCLOSURE

In certain circumstances, the Law allows personal data to be disclosed without the consent of the Data Subject.

Under these circumstances, the Hall will disclose the requested data. However, the Data Protection Representative will ensure that the request is legitimate, seeking assistance from Legal Advisors or Regulators, as necessary.

16.0 TRANSPARENCY

The Hall aims to ensure that individuals are aware that their personal data is being processed and that they understand:

A. What data is being processed
B. Why it is being processed
C. How the data will be used
D. How it will be stored
E. How to exercise their rights

To this end, the Hall has a number of specific Privacy Notices, which are published on the Tullynessle & Forbes website - http://www.tullynessleandforbeshall.co.uk/Governance/GDPR

17.0 VERSION CONTROL

VERSION	DATE	DETAILS	AUTHOR/OWNER
1.0		FIRST DRAFT	Gloria Malcolm