

DATA PROTECTION POLICY

CONTENTS

1. Introduction	1
2. Fassnidge Asset Enterprises Ltd (FAME).....	2
3. Registration with the Information Commissioner’s Officer	2
4. Personal data held	2
5. Data security and maintenance of records.....	6
6. CCTV	8
7. Risks	8
8. Reporting of data breaches.....	9
9. Right of access	10
10. Right to rectification and data quality.....	10
11. Right to erasure including retention and disposal	10

1. INTRODUCTION

The Fassnidge Memorial Trust (the Charity) is a registered Charity set up with a bequest from the Fassnidge Family and exists to provide financial assistance to poor and deprived people in the Hillingdon area. This includes awarding grants to individuals or organisations in need, resident in the London Borough of Hillingdon, and supplying Christmas Hampers. The Charity does not solicit donations from the public instead using its own assets to fund its activities.

This Policy covers how the Charity acts to protect personal data and how the Charity complies with the requirements of the UK General Data Protection Regulation (hereafter referred to in this document as “GDPR”). It also covers the Policy for use of CCTV. The Policy will be updated and approved by the Trustees annually.

Although not required due to the nature of the Charity the Trustees have appointed one of the Trustees, Kelly Martin, as data protection officer (DPO). The DPO is responsible for reviewing and recommending the Charity’s Policy for data protection to the Trustees, for monitoring the Charity’s compliance with GDPR and for reporting any data breaches. The Trustees are responsible for ensuring the Charity complies with GDPR, for annual approval of the Policy and for ensuring compliance with the Policy. The

Trustees, their Advisors¹ and Employees² understand their responsibilities with regards to data protection as set out in this Policy. The DPO and the Accountant have provided detailed briefings at the regular Trustee meetings covering data protection and this will be repeated on an annual basis at the time of refresh of this Policy. Employees will be given training on commencement of their employment and annually thereafter.

This policy will be circulated to all Trustees, and to Advisors and Employees with access to personal data. It should be read in conjunction with the relevant provisions of the Staff Handbook Policy.

2. FASSNIDGE ASSET ENTERPRISES LTD (FAME)

FAME is a dormant company set up by the Charity in the event that a company was required in the future. FAME has not been used and has remained inactive since inception. As such the Accountant has notified the ICO that registration of FAME for data protection purposes is not required and this notification will be refreshed annually. In the event that FAME is used in the future this status will be reviewed.

3. REGISTRATION WITH THE INFORMATION COMMISSIONER'S OFFICER

The Charity registered with the Information Commissioner's Office (ICO) for the purposes of GDPR in October 2018 and will continue to refresh its registration annually. This is the responsibility of the Accountant to the Charity who will confirm completion to the Trustees as part of the Policy refresh.

The Charity's registration number with the ICO is ZA466500.

4. PERSONAL DATA HELD

An information audit has been completed by the Charity to identify personal data held, where it originates from and the purpose for which the Charity holds that data.

¹ Advisors as referred to in this Policy means the Charity's Legal Advisor Frazine Johnson and the Charity's Accountant Fiona Morgan. No other Advisors of the Charity have access to any personal data.

² Employees means employees of the Charity either directly employed by the Charity or on a self-employed basis.

The Charity holds personal data on individuals and organisations necessary for the Charity to comply with the requirements of:

- 1) the Charities Commission;
- 2) any government or other legal requirement;
- 3) the Charity's own governing documents;
- 4) production of the audited financial report and accounts including information requested or likely to be requested by the Charity's Auditors; and
- 5) information required to allow the Charity to fulfil its objectives of providing financial assistance to poor and deprived people in the Hillingdon area.

The personal data held by the Charity is not shared with anyone or any organisations other the Trustees, the Advisors, the Employees or the Charity's Auditors for the purposes of the annual audit or independent examination of the financial report and accounts.

The Charity's Auditors are expected to safeguard the information supplied to them for the purposes of the audit of the financial report and accounts in accordance with their own data protection policy and duty of confidentiality. A copy of this Policy is supplied to the Charity's Auditors.

The Charity holds the following types of personal data:

4.1 Trustees, Advisors and Employees

Certain personal information is held including names, addresses, emails and other data. The Trustees and Advisors confirm by their approval of this policy their consent for the Charity to hold this information. Employees will be requested to confirm their consent. As stated above this policy should be read in conjunction with the Staff Handbook Policy.

Information on Trustees who have resigned from the Charity is held only so far as this is necessary to satisfy the requirements listed in Section 4 of this document.

4.2. Grant information

In accordance with the Charity's Policy for Grants, organisations applying for grants on behalf of individuals are required to supply the Charity with various personal data on those individuals. This information includes but is not limited to the following:

- Name
- Age
- Address
- Employment status
- Income
- Benefits received
- Housing status
- Health conditions
- Other data as required

The information above is required to allow the Trustees to properly assess the grant applications to determine the extent to which approving or partially approving the grant would be within the terms of the governing document of the Charity and, also how the application compares with other applications received, to ensure maximisation of the available resources of the Charity.

In addition the Charity's Policy for Grants states that individuals are not eligible to receive more than one grant in total from the Charity and therefore a register is maintained of applicant name, address and details of any grant awarded to ensure that grants are not awarded to any applicant that has received a grant in the past irrespective of the time period that has elapsed since the previous grant. As the Charity by its governing documents will continue in perpetuity this information will be held in perpetuity.

The grant application form required to be completed for all grant applications contains guidance notes on the Charity's maintenance of personal data and the reasons why this data is kept and notes that the applicant and the organisation applying for the grant consent to the Charity holding the information necessary.

4.3 76 High Street Northwood & Kate Fassnidge Community Hall Uxbridge

The Charity owns the freehold of a property - 76 High Street Northwood - containing a community hall, the Kate Fassnidge Community Hall Northwood (KFCH Northwood) and 8 flats. The Charity also owns the leasehold of the Kate Fassnidge Community Hall Uxbridge (KFCH Uxbridge).

The Charity hires out the KFCH Northwood and the KFCH Uxbridge to the local community including to individuals. Personal data is kept to a minimum comprising name, address, email if applicable and bank account details to allow refund of deposit. This information is supplied by the person hiring the hall on the relevant Hall booking form. The Hall booking form includes notes on the Charity's maintenance of this data and notes that the person hiring the Hall consents to the Charity holding this information.

Where issues have arisen resulting from the hire such as non-payment of hire fee, issues with the condition of the Hall after the hire, or damage done then a record will be kept so that decisions as to any future hire can be made with the relevant information known.

The leasehold owners of the 8 flats pay ground rent to the Charity on an annual basis. The Charity maintains a register containing the names, addresses and emails of the owners to allow invoices for the ground rent due to be sent. This information is maintained by the Accountant. The Legal Advisor, who is separately registered with the ICO, also holds the leases and other information relating to the flat owners. The Employees and Trustees also have access to this information where required to ensure payment of ground rent or proper maintenance of the property.

4.4 Other activities of the Charity

The other activities of the Charity do not involve the Charity holding any personal data other than email addresses for key contacts who work with the Charity in various capacities. The Charity also holds the names of event attendees for the purposes of its guest lists.

Christmas hampers are supplied only to organisations who distribute them to individuals of their own choice. The Charity is not informed of the identity of the individuals who receive the hampers. The Charity does receive letters of thanks or photographs from some recipients on an unsolicited basis. Where this is the case letters of thanks received will be communicated to the Trustees before being destroyed. Photographs may be used on the Charity's website where permission is received from the individual(s) but no names are disclosed or maintained.

The Charity rents property to Trinity Homeless Projects who sublet to formerly homeless individuals. The Charity is not advised of the identity of the individuals living in the property.

5. DATA SECURITY AND MAINTENANCE OF RECORDS

Data is held mainly by the Charity's Legal Advisor, Accountant and Employees in both electronic and hard copy format. The remaining Trustees have access to personal data only as far as is required for the purposes specified in section 3 above.

5.1 Trustees and Advisors

The data and records relating to meetings are held securely by the Charity Manager for 7 years after which it is destroyed. The Minutes of the Trustees' meetings and policies etc along with all documents of an official nature necessary for running the Charity are maintained indefinitely in a secure cabinet. The Accountant and Charity Manager also maintain records only as required for the performance of their roles.

5.2 Grant applications

Grant applications are usually sent to the Employees acting as Charity Manager via email using the administrator email address set up by the Charity. Access to the administrator email is restricted to the Charity Manager, and certain Trustees as necessary.

The Charity's Policy for Grants which forms part of the application form for grants clearly states that all grant applications sent must be either password protected or encrypted and no mention of the applicant name or other applicant details should be made in the body or title of the email. Whilst encryption is preferred password protection is also permitted given the voluntary nature of some of the organisations requesting grants on behalf of individuals. Where password protection is used the password must be notified via email on a separate email to the application. Use of encryption or password protection is the responsibility of the applicant organisation and the Charity is not responsible for ensuring this.

Once the application is received the Charity Manager will acknowledge receipt and allocate a code number to the application which should be used in all further correspondence, with the initials of the applicant, concerning the application.

A soft copy of each grant application and other relevant information is kept by the Charity Manager on a Charity supplied computer. Maintenance of these records are required to ensure grants are settled and for audit purposes.

A register of grants, together with details of orders placed are maintained, in spreadsheet format, for each year by the Charity Manager and the Accountant. All versions of the spreadsheet are password protected and are stored on the Charity's network only.

Where grants require the purchase of items from AO or other supplier organisations, the name, address and phone number of the person receiving the grant are supplied to the supplier organisations to enable goods ordered to be delivered. Details of orders and addresses will be held by the supplier organisation and security of these records are the responsibility of the supplier organisation.

5.3 KFCH Northwood and KFCH Uxbridge

The booking forms for hiring of the Halls includes a provision requiring the person hiring to give explicit permission for the personal data supplied to be used in order to process the application and for the information to be kept for the purposes of the audit of the financial statements of the Charity. The booking form also requires the person hiring to allow maintenance of the records for a longer period in the event of any issues during the hire.

Booking forms are managed by the Charity Manager and are kept in hard or soft copy depending on how they are received from the person requesting the Hire.

Only where there are issues with the Hire are names and addresses kept after the completion of the audit of the financial statements for the year of the hire and settlement of any hire fee or deposit refunds.

Certain individuals/organisations hire the Halls on a regular basis. Where this is the case invoices are usually sent via email with details of hire charges due. Invoices are held by the Charity Manager electronically on the Charity's network.

Details of the leaseholders for the purposes of ground rent invoices are held by the Charity Manager electronically on the Charity's network are subject to the controls described above. Invoices are sent by email.

Information held by the Accountant in order to maintain the books and records of the Charity for the purposes of the Audit of the Annual Accounts are maintained on the personal computer of the Accountant and are password protected. Access to the computer is also password protected. In the event that the Computer will no longer be used all files containing personal information will either be transferred to the Charity's shared drive or deleted.

6. CCTV

The Charity commissioned a third party Octagon Ltd to install CCTV cameras outside 76 High Street Northwood & KFCH Uxbridge to protect the property of the Trust. The cameras are positioned to capture people approaching the entrances to each Hall. The cameras at KFCH Uxbridge do not point at any roads and therefore no vehicles are captured on the system. For KFCH Northwood, due to the configuration of the area a small stretch of the High Street, immediately adjacent to the Hall, is captured by the CCTV but due to positioning of the cameras it is difficult, but not impossible, to read vehicle registration numbers. Information is posted at both Halls to notify Hall users that CCTV is set up outside the Halls.

The CCTV equipment at both halls is located behind locked cupboard doors and is only accessible to keyholders being the Trustees and Employees responsible for Hall Hire. A password is also required to access the system. Octagon Ltd have no access to the CCTV tapes. The images recorded by the CCTV are streamed to the Charity's Office and access to the system is restricted by password. Review of images will only be done in the event of damage, or suspected attempt to cause damage, to the Charity's property or to people using the Hall, or if requested by the Police. Details of the reason for the review and of the images reviewed will be logged by the Charity Manager and brought to the attention of the Trustee responsible and the Charity's DPO. Review of the CCTV will not be undertaken for any other reason. The tapes are overwritten once full and are not retained.

7. RISKS

The DPO and the Trustees have assessed the risks of personal data leakage and consider the material risks to be as follows:

1. Leakage of personal data through theft of papers or computers;
2. Leakage of personal data through unauthorised access to emails;
3. Leakage of personal data through listening to conversations or meetings; and
4. Misuse of the CCTV equipment.

The DPO and the Trustees consider the mitigants against the material risks identified to be as follows:

1. Password protection of all files containing personal data with the password for files internal to the Charity. For personal data sent in password protected files to the Charity, the sending organisation will be responsible for setting and supplying a password;
2. The Charity endeavours to minimise the amount of printed personal data. However, to allow the Trustees to properly assess grant information, for maintenance of Hall booking records and for the Annual Audit some printed data is used. This will be kept as securely as possible and destroyed by shredding as soon as no longer required;
3. Printed data when transported to meetings and computer equipment may be subject to theft. Where computer equipment is stolen some protection is given by password protection of files. The Charity will take all possible steps to safeguard equipment and papers but some level of risk is deemed to be unavoidable;
4. Organisations sending applications to the Charity are assumed to be responsible for data protection for information sent until received and actioned by the Charity. Access by the Charity to email is password protected. There are no other steps that the DPO and the Trustees consider practical to protect email communication;
5. For Hall booking and invoicing purposes email communication is used and this will continue as the only practical method of organising bookings; and
6. CCTV is only accessible by password retained by the Trustees responsible and by the Charity Manager and tapes will only be reviewed as specified in section 6 above.

8. REPORTING OF DATA BREACHES

The Trustees and their Advisors are individually responsible for reporting unauthorised access to personal data to the DPO. The DPO is then responsible for reporting the data breach to the ICO and for notifying the Trustees that such notification has been made. A log of any data breaches will be maintained by the Charity Manager.

Where a data breach has occurred the DPO and the Trustees collectively are responsible for considering the root cause of the breach and whether any steps are required to strengthen the Charity's Policy and processes for data protection to avoid re-occurrence.

As at the date of approval of this Policy no data breaches have been identified by the Charity.

9. RIGHT OF ACCESS

Individuals are entitled to be notified of their own personal data held by the Charity. Requests for personal data received in writing to the Charity will be notified to the Trustees, who will decide which

method of notification should be followed to transmit the information to the requestor. The notification to the requestor will be actioned by the Charity Manager. The Charity Manager will take all steps possible to ensure that the identity of the person requesting the information is verified prior to sending the information.

As at the date of approval of this Policy no requests for personal data have been received by the Charity.

10. RIGHT TO RECTIFICATION AND DATA QUALITY

Where individuals have been notified of their personal data held by the Charity and as a result advise the Charity of a change required to that data, the Trustees will consider the request and, provided they agree the request is valid, will request that the person holding the relevant electronic record to immediately amend this data and notify the Trustees as a body that this has been done. The DPO will be responsible for monitoring completion.

The person requesting the change will be notified of the action taken and where the change is not considered as valid by the Trustees will be advised of this and the reason why.

The Charity will take care that the data held is accurately maintained bearing in mind that the information is not used by the Charity to approach individuals directly other than as agreed by the individuals concerned.

11. RIGHT TO ERASURE INCLUDING RETENTION AND DISPOSAL

The Policy covers the reasons for retention of personal data above and considers retention of this data to be required to allow the Charity to fulfil the aims of its governing document.

All printed data will be disposed of by shredding. Deletion of computer files no longer required will include deletion from all forms of storage.

GDPR Policy reviewed September 2023