POLICY

DATA PROTECTION

In this Policy and its Procedures, the term "Barnaby Team" or "Barnaby Team member" refers to any person MBF have appointed to help organise events/exhibitions/activities, whether volunteer or paid, and all relevant contractors.

POLICY STATEMENTS:

- All information sought or gathered or held by MBF will meet the requirements of the 8 Data Principles of the Data Protection Act 1998 and will be gathered and used solely for the purposes of running the Festival.
- The only Personal data recorded will be data that is of use in either running the Festival, complying with legal requirements, or providing information to funding bodies. This data may include Sensitive Personal data.
- Personal data will only be captured with the consent of the individual.
- Specific items of data will only be used for the purposes for which they were given.
- Personal data will be shared with other organisations only as needed for the purpose of running the Festival.
- Where relevant to the duties of the role, contracts and agreements will state that compliance with this DP Policy and Procedures is required.
- The setting up of any new database or other electronic record containing personal data must be approved by the Board of Trustees.
- Personal data will be held on file only for as long as required. Decisions about how long different types of data will be held will be defined by the MBF Information Governance Policy.
- Documents containing lists of Personal Data should not be shared via Gmail, Yahoo, Hotmail or similar email accounts but instead be shared via Dropbox.
- Team members handling Personal Data will receive appropriate data protection training.
- The Board will keep under review the need for MBF to register as a Data Controller.
- The Board will keep under review the implications of holding data on servers outside the UK.
- Any breach of data protection rules will be notified to the Data Protection Registrar and to all individuals affected.

PROCEDURES:

- 'Personal' and 'Personal Sensitive' data is defined by the Act *(see p2)*
- all Personal information will be held in password-protected electronic files wherever possible. Where people provide details on paper, Barnaby team members should enter those details into the relevant secure database as soon as is practical and then shred the paper record. This includes sign-in sheets at volunteer meetings.
- where the method of consent is not automatically recorded by the relevant software, Barnaby team members will add a record of the source of the personal data to the database concerned.
- all team members will take care to keep Personal Data secure when it is being used outside a password-protected database (e.g. when volunteers are given contact details of other volunteers as needed for the organisation of the festival).

- team members issued with Barnaby email addresses should access their email only through a password protected email client or device
- team members working with password protected files must always log out as soon as the task is complete.
- all passwords will contain upper and lower case letters, a number and a symbol (where allowed for by the software concerned).
- wherever possible, individual rather than shared passwords will be used.
- a record of shared passwords will be kept within a Dropbox folder document to which only trustees and central office team members are invited.
- shared passwords will be changed in the October of every year. This task will be added to the Board agenda for each October board meeting so it can't be overlooked.
- a record of who has access to which password protected software and what their role is will be kept in a Dropbox folder to which only trustees and central office team members are invited. At the time of writing, this folder is MBF Central/Admin/Database Access log. The log will be managed by a trustee.
- before being authorised to use or create a database containing Personal Data, new users must:

    a) sign a volunteer agreement form, contract for services, or contract of employment
    b) be taken through the Data Protection principles
    c) read the Barnaby Festival DP policy & procedures
    d) be approved by two trustees
    e) be recorded in the database access log

- decisions about who to authorise will be based on trustees' best judgement.
- where there is a shared password and a team member leaves the team using this password, the team leader will organise a password change via a trustee. Add this as to operational plan as an action.
- team members must not link software such as MailChimp to their own personal accounts for the software concerned. This is because password changes may not in this scenario terminate user access.
- Documents containing personal data should not be emailed via webmail accounts such as hotmail, google, yahoo etc.
- the website and any web page requesting Personal Data will contain a link to a privacy policy.
- in the event of a breach, the person first becoming aware of the breach should notify the Board and the central office team. The response to the breach will be co-ordinated by a trustee, normally the trustee responsible for the Data Protection Policy. The first step will be to change any relevant passwords. Other steps will include notifying affected individuals and the ICO.
- MBF will provide appropriate training for team members starting a role that involves working with Personal Data and will hold an annual data protection training refresher session for all relevant team members.
- any subject access requests received will be passed to the trustee responsible for the Data Protection Policy. He or she will request ID details from the individual and check these to ensure data is only released to the individual concerned.

  Once ID details have been approved, he or she will investigate what information is held and ensure a full response is provided to the individual within the 40 days required by the Act.

  This response will include: whether any personal data is being processed; a description of the personal data, the reasons it is being processed, and whether it has been or will be given to any other organisations or people, a copy of the information comprising the data; and details of the source of the data (where it is available). In handling subject access requests, MBF will use the ICO checklist at

  https://ico.org.uk/for-organisations/subject-access-request-checklist

  A fee of £10 will be levied. This cost will be advised to the individual at the time of receiving their request.

AGREED BY THE MBF BOARD OF TRUSTEES.....25 May 2017

REVIEW.....April 2018 or earlier if new legislation comes into force before that date.

APPENDIX re DATA PROTECTION

The 8 Data Protection Principles

The Data Protection Act controls how personal information is used by organisations, businesses or the government. Everyone responsible for using data has to follow the 8 Data Protection Principles.

They must make sure the information is:

- used fairly and lawfully
- used for limited, specifically stated purpose(s)
- used in a way that is adequate, relevant and not excessive
- accurate and up to date
- kept for no longer than is absolutely necessary for the stated purpose(s)
- handled according to people's data protection rights
- kept safe and secure to avoid loss or damage
- not transferred outside the UK without adequate protection

The data subject must give permission for data to be gathered/processed/held in the way that is described to them at the time. Explicit consent must be given for the processing/holding of Personal or Sensitive Personal information.

PERSONAL DATA means data which relate to a living individual who can be identified from those data. This includes:
names, contact details and photos a well as more detailed data about the person such as expressions of opinion (as in a performance review, for example) or information about what is going to happen to that person, training records, contracts, details of people's finances, expenses or pay, decisions made on leadership or responsibilities given, and why;

SENSITIVE PERSONAL DATA means personal data, including images, consisting of information as to ethnic origin, political opinions, religious beliefs, trade union membership, physical/mental health/ condition, sexual life, criminal records. It may also include such data as where children go to school or take part in leisure activities, concerns for welfare, accident reports, comments on home difficulties, duties as a carer, etc

There is stronger legal protection for Sensitive Personal data

Note: reasons MBF may hold Sensitive Personal data include providing data to funders e.g. ethnicity quotas