EAST MALLING INSTITUTE TRUST

Data Protection Policy and Procedures

Background

In order for the East Malling Institute Trust to manage the Institute Hall, its hirings and finances, it is inevitable that we will need to collect and use personal data. It is our responsibility to ensure that the data collected is used only for this purpose and to ensure that the data we hold is kept secure. Protecting the rights and privacy of individuals, in line with Data Protection laws and regulations, is very important to us.

The Data Protection Act 1998 (DPA) and General Data Protection Regulations (GDPR) govern the use of information about people (personal data). Personal data may include e.g. names, addresses, telephone numbers and email addresses, and may be held in a variety of ways including on computers, laptops and mobile devices, or in hard copy form. Data may be included in such things as emails, minutes of meetings, booking forms, and photographs.

Under legislation EMIT is the Data Controller for the information held. The Trustees, volunteers (including Management Committee Members) and staff are responsible for processing and using personal information in accordance with the Data Protection Act and GDPR.

Trustees, volunteers and staff who have access to personal information will therefore be expected to read and comply with this policy.

Our Responsibilities

EMIT is committed to adopting best practice for the protection of personal data. Trustees place a very high degree of importance on the lawful and correct treatment of personal information which is vital to maintaining the confidence of those entrusting us with that data. We recognise the risks to individuals of identity theft and potential financial loss if personal data is lost, stolen or destroyed. This policy sets out the steps we take to minimise that risk.

The East Malling Institute Trust, as a Data Controller under the Act, is legally responsible for complying with Act. It also means that EMIT determines the purposes for which personal information held will be used.

In order to meet its responsibilities under the Act EMIT will:

a) Collect and use information fairly and lawfully;
b) Specify the purposes for which information is used - that is for the purpose of managing bookings by our hirers and managing our finances;
c) Collect and process appropriate information, and only to the extent that it is needed to fulfil our operational needs or to comply with any legal requirements;
d) Ensure that the data we hold is accurate and kept up to date and is held for no longer than necessary;
e) Ensure the rights of people about whom information is held can be exercised under the Act. These include:
    i) The right to be informed that processing is undertaken;
    ii) The right of access to one's personal information;
    iii) The right to prevent processing in certain circumstances, and
    iv) The right to correct, rectify, block or erase information which is regarded as wrong information;
f) Safeguard personal information by implementing suitable security measures to minimise the risk of unlawful processing, accidental loss, destruction or damage to personal data ;
g) Ensure that personal information is not transferred abroad without suitable safeguards;

h) Treat people justly and fairly whatever their age, religion, disability, gender, sexual orientation or ethnicity when dealing with requests for information;
i) Set out clear procedures for responding to requests for information.

All Trustees, staff and volunteers are aware that a breach of the rules and procedures identified in this policy may lead to action being taken against them.

Policy Implementation, and Measuring and Reviewing Effectiveness

EMIT is not required under the legislation to appoint a Data Protection Officer.

The Trustees, assisted by the Management Committee, will take into account legal requirements and ensure that this policy is properly implemented. The Trustees and Management Committee have determined the processes and steps that should be taken to ensure compliance with legislation and to review the effectiveness of those measures. Full details are provided in EMIT's 'Policy and Procedure for Handling Data and Data Security'.

The Chairman, as the point of contact for any data protection issues or queries, will take steps on behalf of EMIT to resolve any data issues and, including the seeking of any external advice or support as necessary. The Chairman will report to the Trustees and Management Committee in line with EMIT's policy.

Rights of Individuals

Individuals have a right to make a Subject Access Request (SAR) to find out whether we hold their personal data, where we hold it, and what it is used for, including how that data might be shared with others. They have a right to have data corrected if it is wrong, to prevent use which is causing them damage or distress, or to stop marketing information being sent to them.

A SAR must be made in writing but this could be be letter or email. The request must be dealt with within 40 calendar days, although before we can proceed with a SAR request and provide information we must confirm the identity of the individual making the request. They may be asked to provide both photo identification e.g. a passport, and confirmation of address e.g. a recent utility bill, bank or credit card statement.

Anyone wishing to make a Subject Access Request should contact:

Michelle Tatton, Chairman email: michelle.tatton@aol.com 01732 521889

EAST MALLING INSTITUTE TRUST

Policy and Procedure for Handling Data & Data Security

EMIT has a duty to ensure measures are taken to prevent:

- Unauthorised or unlawful processing of personal data
- Unauthorised disclosure of personal data
- Accidental loss of personal data

Trustees, volunteers and staff must ensure that personal data is dealt with properly no matter how it is collected, recorded or used. This applies whether or not the information is held on paper, on a computer or recorded by some other means e.g. tablet or mobile phone.

Personal data relates to data of living individuals who can be identified from that data. EMIT recognises that misuse of that data could cause an individual damage or distress. This does not mean that mentioning someone's name in a document comprises personal data; however, combining various data elements such as a person's name, and salary or religious beliefs etc. would be classed as personal data, and falls within the scope of the DPA. It is therefore important that all those holding and processing data on behalf of EMIT consider any information (which is not otherwise in the public domain) that can be used to identify an individual as personal data and observe the guidance given below.

Consent Forms

Consent forms to enable EMIT to hold and process data will be stored by the Secretary and/or Booking Secretary in a securely held electronic or paper file.

Email and Post

Trustees, volunteers and staff will consider whether an email (both incoming and outgoing) needs to be kept as an official record and, if so, for how long. If the email needs to be retained it should be saved into the appropriate folder or printed and stored securely.

Importantly, emails containing personal information no longer required for operational use, should be deleted from the personal mailbox and any "deleted items" box.

Beware of spam email and emails that would infect your computer or other device with malware/ spyware. Do not be tricked into providing information to which a person is not entitled.

When sending items by post take care to ensure they are properly addressed and envelopes are securely sealed.

Phone Calls

Phone calls can lead to unauthorised use or disclosure of personal information and the following precautions should be taken:

- Personal information should not be given out over the telephone unless you have no doubt as to the caller's identity or that the information requested is innocuous;
- Do not leave personal information on someone's answerphone;
- If you have any doubts, ask the caller to put their enquiry in writing;
- If you receive a phone call asking for personal information to be checked or confirmed be aware that the call may come from someone impersonating someone with a right of access;
- If someone leaves personal information on your answerphone that this is transferred at the earliest opportunity to safe storage (assuming it is data to be held by EMIT) and the answerphone message is deleted;

Computers, Laptops and Portable Devices

All computers/laptops/portable devices/mobile phones that hold data containing personal information **must** be protected with a password, firewall, and anti-virus/malware software.
You must ensure that your devices are locked/password protected when left unattended, even for short periods of time.
If you take your laptop/portable device with you in the car make sure it is out of sight, preferably in the boot.
If you have to leave a laptop or portable device in an unattended vehicle at any time, put it in the boot and ensure all doors are locked and any alarm set.
Never leave laptops or portable devices in your vehicle overnight.
Do not leave laptops or portable devices unattended in restaurants or bars, or any other venue.
When travelling on public transport, keep your portable devices with you at all times. Do not leave them in luggage racks or even on the floor alongside you.

Data Security and Storage

Store as little personal data as possible on your computer or laptop. Only keep those files that are essential. Personal data received on disk or memory stick should be saved to the relevant file on the computer/laptop etc. The disk or memory stick should then be securely returned (if applicable), safely stored or wiped.
Always lock/password protect your computer, laptop or portable device when left unattended.

Passwords

Do not use passwords that are easy to guess. All your passwords should contain both upper and lower-case letters and preferably contain some numbers and other characters. Ideally passwords should be 8 characters or more in length.

Protect Your Password

Common sense rules for passwords are:

Do not give out your password to anyone
Do not write your password somewhere on or near your laptop, computer or other portable device

Data Storage

- Personal data will be stored securely and will only be accessible to authorised Trustees, volunteers or staff.
- Information will be stored for only as long as it is needed or required by statute and will be disposed of appropriately. Accounting/financial records will be kept for up to 6 years. For employee records please see below. Archival material such as Minutes and legal documents will be stored indefinitely. Other correspondence and emails will be disposed of when no longer required or when Trustees, volunteers or staff retire. Paper records will be disposed of by shredding.
- All personal data held for the organisation must be non-recoverable from any computer which is disposed of/passed on/sold to a third party.

Information Regarding Employees or Former Employees

Information regarding an employee, or a former employee, will be kept indefinitely. If something occurs years later it might be necessary to refer back to a job application or other document to check what was disclosed earlier, in order that Trustees comply with their obligations e.g. regarding employment law, taxation, pensions or insurance.

Accident Book

The accident book will be checked regularly. Any page which has been completed will be removed, appropriate action taken and the page filed securely by the Chairman.

Sharing Data

We regard the lawful and correct treatment of personal information as very important to successful working, and to maintaining the confidence of those with whom we deal. We will always strive to ensure that personal information is treated correctly.

We may occasionally need to share data with other agencies such as the local authority, funding bodies and other voluntary agencies in circumstances which are not in furtherance of the management of the charity. While data would not ordinarily be shared without the data subject's consent, the circumstances where the law allows the charity to disclose data (including sensitive data) without the data subject's consent are:

- Carrying out a legal duty or as authorised by the Secretary of State Protecting vital interests of a Data Subject or other person e..g. child protection The Data Subject has already made the information public
- Conducting any legal proceedings, obtaining legal advice or defending any legal rights
- Monitoring for equal opportunities purposes – i.e. race, disability or religion.

Subject Access Requests

A Subject Access Request (SAR) allows an individual to find out what personal data is processed by EMIT, where that data is held, and what it is used for, including how that data might be shared with others. There is a right to have data corrected if it is wrong.

EMIT has determined that SARs will be handled by the Chairman. In handling the request, the Chairman will consider:

- **Proof of identity:** this may be required in the form of photo ID (e.g. passport) and proof of address e.g. a recent utility bill;
- **Fee:** The maximum fee is usually £10;
- **The Information:** If the information is available tell the requester as soon as possible, and within the 40 day calendar period. If it includes information about other people you will not have to supply the information unless the other people have given their consent for disclosure or it is reasonable to supply the information without their consent. If it is not appropriate to disclose other people's data, disclose as much information as possible by redacting references to them;
- **Exempt Information:** If information is exempt, tell the requester as soon as possible. If it not necessary to say why the data cannot be revealed. However, this is unlikely to apply in the case of EMIT held data.

The Chairman will report all SARs to the Trustees and Management Committee for noting.

Data Breaches

We will take any misuse, theft, loss or destruction of personal data very seriously. If a data breach occurs the Chairman should be informed immediately so that he/she can conduct an investigation and report the to the Trustees and Management Committee. Our process will include:

- Notifying the person whose data has been affected, explaining what has happened and advising what we intend to do next;
- Carrying out an investigation to find out why the breach happened and to determine what can be done to prevent it happening again. As necessary the Chairman will seek external advice and support;
- Reporting by the Chairman to the Trustees and Management Committee of any arising data protection issues;
- Ensuring any necessary measures are implemented as soon as possible;
- In the event of a serious breach, reporting the matter to the Information Commissioner

Risk Management and Review

The consequences of breaching Data Protection can cause harm or distress to service users if their information is released to inappropriate people, or they could be denied a service to which they are entitled. Trustees, volunteers and staff should be aware that they can be personally liable if they use customers' personal data inappropriately. This policy is designed to minimise the risks and to ensure that the reputation of the charity is not damaged through inappropriate or unauthorised access and sharing.

The Trustees and Management Committee will carry out an annual review of the effectiveness of this policy. That review, which will be considered at the first meeting after the Annual General Meeting, will:

a) Ensure that everyone processing personal information understands what is required under this policy and that they are responsible for following good data protection practice;
b) Ensure that anybody wishing to make enquiries about handling personal information knows what to do;
c) Ensure any enquiries about handling personal information are being dealt with promptly and courteously;
d) Review the way in which EMIT is holding, managing and using personal information and update its Data Map and processes as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments made to the data protection legislation.

If you have any queries regarding this policy please contact:

Michelle Tatton, Chairman email: michelle.tatton@aol.com 01732 521889

Definitions

The following are definitions of the terms used:

Data Controller
The trustees who collectively decide what personal information EMIT will hold and how it will be held or used.

Act
The Data Protection Act 1998 and General Data Protection Regulations - the legislation that requires responsible behaviour by those using personal information.

Data Protection Officer
The person responsible for ensuring that EMIT follows its Data Protection Policy and complies with the Act. [EMIT is not required to appoint a DPO].

Data Subject
The individual whose personal information is being held or processed by EMIT, for example a donor or hirer.

'Explicit' consent'
This is a freely given, specific agreement by a Data Subject to the processing of personal information about her/him.
Explicit consent is needed for processing "sensitive data", which includes:
(a) Racial or ethnic origin of the data subject
(b) Political opinions

(c) Religious beliefs or other beliefs of a similar nature
(d) Trade union membership
(e) Physical or mental health or condition
(f) Sexual orientation
(g) Criminal record
(h) Proceedings for any offence committed or alleged to have been committed
EMIT will not generally hold sensitive personal data.

Information Commissioner's Office (ICO)
The ICO is responsible for implementing and overseeing the Data Protection Act 1998.

Processing
This means collecting, amending, handling, storing or disclosing personal information.

Personal Information
This information about living individuals that enables them to be identified e.g. names, addresses, telephone numbers and email addresses. It does not apply to information about organisations, companies and agencies but applies to named persons, such as individual volunteers.

EAST MALLING INSTITUTE TRUST

Privacy Notice and Consent Policy

This privacy notice sets out why EMIT requires your data, and how it collects, stores, and uses personal information. It describes:

Why We Require Your Data and How We Collect It

It is necessary for us to collect personal information from you when you make an enquiry or a booking, whether this is by telephone, email or through our website. We will also need to collect data from you if you offer your services as an EMIT volunteer, or if you are an employee.

When you contact us about a booking we will obtain sufficient information to enable us to proceed with your enquiry and for us to be able to contact you. If you enter an agreement to hire the Hall, or part of it, you will be asked to complete a Booking Form and provide details for us to be able to invoice you.

How Your Data Will Be Stored and Used

When you provide us with personal data we will only use it for the purpose for which it was provided.

We may share all or part of your personal data with Trustees, members of the Management Committee, volunteers, contractors and suppliers insofar as this is reasonably required to enable efficient management of your booking or enquiry.

We will not share your data with third parties without your consent or unless we have a legal obligation to do so.

We will never sell your data.

When you fill in a Booking Form that document becomes part of our financial records which we are required to keep for 6 years for accounting purposes.

Data Collected Through Our Website

When you visit our website at www.eastmallinginstitutehall.co.uk the website automatically records details of visitor behaviour patterns. This helps us to see how many visitors various pages within our website have attracted. The information collected is anonymous and we are unable to identify users from this activity.

When you contact us through our website your details are forwarded to our Web Administrator who will direct the email to the person most able to help with your enquiry. Your message is not stored within the website.

Our website does not use cookies.

We are not responsible for the content of any linked websites.

You can find out more about how we handle personal data by reading our Data Protection Policy and Procedures.

If you wish to make a Subject Access Request please contact:

Michelle Tatton, Chairman email: michelle.tatton@aol.com 01732 521889