Data Protection Policy

Milton Keynes Heritage Association is committed to continual development and improvement of its data protection practice through review of its policies and procedures

BACKGROUND

The Association (otherwise referred to as MKHA) was established to encourage and develop cooperation and coordination between all members having an interest in heritage in the area centred on the Milton Keynes Unitary Authority (otherwise Milton Keynes Council). Members are admitted from within the area of the Authority, and at the discretion of the Executive Committee from a wider area.

It is an 'umbrella' organisation overseeing and coordinating heritage related activities amongst its 60 plus individual independent member groups

The objects of the Association fall within the following areas: - Heritage Policy, Collecting Policy, Research/recording of history, Publicity, Education, Training, Communication, Activities, Conservation/ display, Raising funds, Investment of monies, Legal requirements, Grants and projects and Not-for-profit commercial activities.

INTRODUCTION

MKHA needs to gather and use certain information about member groups and individuals in order to fulfil its constituted aims and objectives.

This policy describes how this data is collected, handled and stored to meet MKHA data protection standards, and to comply with current legal requirements.

WHY THE POLICY EXISTS

This data protection policy ensures that MKHA:-

- Complies with data protection law and follows good practice
- Protects the rights of its members, as represented by MKHA Executive Committee
- Is open about how it stores and processes individual and member group data
- Protects itself from the risks of a data breach

DATA PROTECTION LAW

The Data Protection Act 2018 describes how organisations (including voluntary organisations), including MKHA must collect, handle and store personal information.

These requirements apply regardless of whether data is stored electronically, on paper or on other materials.

To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The current legal requirements are underpinned by important principles. They say that personal data must:

- Be processed fairly and lawfully
- Be obtained only for specific, lawful purposes
- Be adequate, relevant and not excessive
- Be accurate and kept up to date
- Not be held for any longer than necessary
- Processed in accordance with the rights of data subjects
- Be protected in appropriate ways
- Not be transferred outside the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection

PEOPLE, RISKS AND RESPONSIBILITIES

POLICY SCOPE

This policy applies to MKHA and will be commended to its members, (including any future employees) and all contractors, suppliers and other people working on behalf of MKHA.

It applies to all data that MKHA holds relating to identifiable individuals. This can include:

- Names of individuals
- Postal addresses
- Email addresses
- IP addresses
- Telephone numbers
- Financial information
- Any other information relating to individuals or member groups

For the purposes of this policy all of the above personal information, whether referred to jointly or severally, or is embedded wholly or partially within another document, is covered by the definition 'Data'.

DATA PROTECTION RISKS

This policy helps to protect MKHA from some very real data security risks, including:

- **Breaches of confidentiality.** For instance, information being given out inappropriately.
- **Failing to offer choice.** For instance, all individuals should be free to choose how MKHA uses data relating to them.
- **Reputational damage.** For instance, MKHA could suffer if hackers successfully gained access to sensitive data.

Responsibilities

Everyone who works for or with MKHA has some responsibility for ensuring data is collected, stored and handled appropriately.

Everyone who handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

However, these people have key areas of responsibility:

- The **MKHA Executive Committee** is ultimately responsible for ensuring that MKHA meets its legal obligations.
- The **MKHA Chairman or other member of the Executive management committee otherwise designated as the MKHA data protection officer,** is responsible for:
    - Keeping the Executive Committee and members updated about data protection responsibilities, risks and issues.
    - Reviewing all data protection procedures and related policies.
    - Arranging data protection training and advice for the people covered by this policy.
    - Handling data protection questions from MKHA members and anyone else covered by this policy.
    - Dealing with requests from individuals to see the data MKHA holds about them (also called 'subject access requests').
    - Checking and approving any contracts or agreements with third parties that may handle the organisation's sensitive data.
- The **MKHA Website Manager** is responsible for:
    - Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
    - Performing regular checks and scans to ensure security hardware and software is functioning properly.
    - Evaluating any third-party services the company is considering using to store or process data. For instance, cloud computing services.
- The **MKHA Secretary** is responsible for:
    - Approving any data protection statements attached to communications such as emails and letters.
    - Addressing any data protection queries from journalists or media outlets like newspapers.
    - Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.

GENERAL STAFF GUIDELINES

- The only people able to access data covered by this policy should be those who **need it for their MKHA related work**.
- Data **should not be shared informally**. When access to confidential information is required, this can be requested from the MKHA Data Protection Manager.
- **MKHA will provide training and guidance** to all members and the Executive Committee representatives to help them understand their responsibilities when handling such data.
- MKHA Executive Committee representatives should keep all data secure, by taking sensible precautions and following the guidelines below.
- In particular, **strong passwords should be used** and they should never be shared.
- **Data files should be encrypted and data devices should also be encrypted.**
- Personal data **should not be disclosed** to unauthorised people, either within MKHA or externally.

- Data should be **regularly reviewed and updated** if it is found to be out of date. If no longer required, it should be deleted and disposed of in an approved manner.

DATA STORAGE.

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the MKHA website manager.

When data is **stored on paper,** it should be kept in a secure place where unauthorised people cannot see it.

These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper or files should be kept **in a locked drawer or filing cabinet**.
- **Data printouts should be shredded** and disposed of securely when no longer required.

When data is **stored electronically**, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

- Data should be **protected by strong passwords** that are changed regularly and never shared between members.
- If data is **stored on removable media** (like a CD or DVD or memory stick – see following point), these should be kept locked away securely when not being used.
- Data should only be stored on **designated and encrypted drives**, and should only be uploaded to an **approved and secure cloud computing service**.
- Personal data files should also be **encrypted**
- Data should be **backed up frequently**. Those backups should be tested regularly, in line with the company's standard backup procedures and to the same level of security as the original data files.
- Data should **never be saved directly** to laptops or other mobile devices like tablets or smart phones.
- All servers and computers containing personal data should be protected by **approved security software and a firewall as well as being encrypted**.
- No personal data will be held on the MKHA website

DATA USE

Personal data is of no value to MKHA unless the organisation can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:

- When working with personal data, Executive Committee representatives should ensure **the screens of their computers are always locked** when left unattended.
- Personal data **should not be shared informally**. In particular, it should never be sent by email, as this form of communication is not secure.
- Personal data must be **encrypted before being transferred electronically**.

- Personal data should **never be transferred outside of the European Economic Area**.
- Members or employees **should not save or retain copies of personal data to their own computers.** Always access and update the central copy of any data.

DATA ACCURACY

The law requires MKHA to take reasonable steps to ensure data is kept accurate and up to date.

The more important it is that the personal data is accurate, the greater the effort MKHA should put into ensuring its accuracy.

It is the responsibility of all Executive Committee representatives who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in **as few places as necessary**. MKHA Executive Committee representatives should not create any unnecessary additional data sets.
- MKHA Executive Committee representatives should **take every opportunity to ensure data is updated.**
- MKHA will make it **easy for data subjects to update the information** MKHA holds about them.
- Data should be **updated as inaccuracies are discovered**.

SUBJECT ACCESS REQUESTS

All individuals who are the subject of personal data held by MKHA are entitled to:

- Ask **what information** MKHA holds about them and why.
- Ask **how to gain access** to it.
- Be informed **how to keep it up to date.**
- Be informed how the company is **meeting its data protection obligations**.

If an individual contacts the company requesting this information, this is called a Subject Access Request.

Subject Access Requests from individuals should be made by email, addressed to the MKHA Data Protection Officer.

The MKHA Data Protection Officer will always verify the identity of anyone making a Subject Access Request before handing over any information.

The Subject Access Request shall be fulfilled within the statutory timescale currently in force.

DISCLOSING DATA FOR OTHER REASONS

In certain circumstances, the Data Protection Act allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, MKHA will disclose requested data. However, the MKHA Data Protection Officer will ensure the request is legitimate, seeking assistance from the MKHA Executive Committee.

PROVIDING INFORMATION

MKHA aims to ensure that individuals are aware that their data is being processed, and that they understand:

- How the data is being used
- How to exercise their rights by:
- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to object

BREACHES

MKHA will put in place plans to detect, report and investigate, and take appropriate action should a breach occur.

COMPLAINTS

MKHA will handle data protection complaints by:

- giving people a way of making data protection complaints
- acknowledging receipt of complaints within 30 days of receipt
- without undue delay, taking appropriate steps to respond to complaints, including making appropriate enquiries, and keeping people informed
- without undue delay, telling people the outcome of their complaints.

DATA AUDIT

MKHA will undertake regular audits of its data holdings (at least two yearly)

Review

The Executive Committee shall regularly monitor and evaluate the effectiveness of this policy in achieving the stated aims. This process shall be undertaken two yearly or sooner and shall aim to seek the views of organisations representing the interests of those groups referred to in this policy.

This is the current copy of this policy

Name: _____

Signature: _____

Position …….

Agreed at the AGM on 28 September 2023 v2 review NL Dec 25