Data Protection and Privacy Policy

Classroom Adventures

1. Policy Statement

Classroom Adventures needs to collect and store personal information in the course of its business operations. This policy describes how data will be collected, handled and stored in order to meet data protection standards, and to comply with current legal requirements.

2. Why this Policy Exists

This Policy ensures that Classroom Adventures:

- Complies with data protection law and follows good practice
- Protects the rights of its staff, volunteers and customers
- Is open about how it stores and processes personal information
- Protects itself from the risks of a data breach

3. Scope

This policy applies to Classroom Adventures: including its staff (including any future employees), volunteers and all contractors, suppliers and other people working on behalf of Classroom Adventures.

It applies to all personal information held by History Adventures, which can include:

- Names of individuals
- Job Titles
- Names of Organisations
- Postal/billing addresses
- Email addresses
- Telephone numbers
- Financial information

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'.

4. Data Protection Law

The General Data Protection Regulation (GDPR) describes how organisations must collect, handle and store personal information. These rules apply regardless of whether data is stored electronically or on paper. 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:

a) processed lawfully, fairly and in a transparent manner in relation to individuals;
b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
d) accurate and, where necessary, kept up to date;
e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;
f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures

5. Data Protection Risks

This policy helps to protect Classroom Adventures from data security risks, including:

- Breaches of confidentiality. For instance, information being given out inappropriately.
- Reputational damage. For instance, History Adventures could suffer if hackers successfully gained access to sensitive data.

6. Responsibilities

Everyone who works for or with Classroom Adventures has 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.

6.1 Key areas of responsibility:

- The business owners are ultimately responsible for ensuring that Classroom Adventures meets its legal obligations.
- The Owners responsible for:
    - Keeping and staff updated about data protection responsibilities, risks and issues.
    - Reviewing all data protection procedures and related policies.
    - Checking and approving any contracts or agreements with third parties that may handle the organisation's sensitive data.
    - Arranging data protection training and advice for the people covered by this policy.
    - Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
    - Evaluating any third-party services the company is considering using to store or process data. For instance, cloud computing services.
    - 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.
    - Dealing with subject access requests.

7. General Staff Guidelines

- The only people able to access data covered by this policy should be those who need it for their History Adventures related work.
- Data should not be shared informally. When access to confidential information is required, this can be requested from the data processor.
- History Adventures will provide training and guidance to all members to help them understand their responsibilities when handling such data.
- Data should be kept secure by taking sensible precautions and following the guidelines below.
- In particular, strong passwords should be used and they should never be shared.
- Files containing data covered by this policy should be password protected.
- Personal data should not be disclosed to unauthorised people, either within History Adventures or externally.
- Data should be regularly reviewed and updated. If it is found to be out of date or no longer required, it should be deleted and disposed of in an approved manner.

8. Data Storage

These rules describe how and where data should be safely stored.

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.

- When not required, the paper or files should be kept in a locked drawer or filing cabinet.
- Data 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, 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 drives, and should only be uploaded to an approved and secure cloud computing service.
- 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.
- All servers and computers containing personal data should be protected by approved security software and a firewall.

9. Data Use

Personal data is of no value to Classroom Adventures 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 staff should ensure the screens of their computers are always locked when left unattended.
- Personal data should not be shared informally.
- Personal data should never be transferred outside of the European Economic Area.
- Personal data should never be saved or retained to the personal computers of staff, volunteers or Trustees. Always access and update the central copy of any data.

10. Data Accuracy

The law requires Classroom Adventures to take reasonable steps to ensure data is kept accurate and up to date. It is the responsibility of all staff, volunteers and Trustees 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. Additional and unnecessary data sets should not be created.
- Staff and volunteers should take every opportunity to ensure data is updated.
- History Adventures will make it easy for data subjects to update the information History Adventures holds about them.
- Data should be updated as inaccuracies are discovered.

11. Subject Access Requests

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

- Ask what information Classroom Adventures holds about them and why.
- Ask how to gain access to it.
- Be informed of how to keep it up to date.
- Be informed of 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 to the Business Owner (info@classroomadventures.co.uk) who will verify the identity of anyone making a Subject Access Request before handing over any information.

12. Disclosing Data for Other Reasons

In certain circumstances, the data protection regulations allow personal data to be disclosed to law enforcement agencies without the consent of the data subject. Under these circumstances, History Adventures will disclose requested data.

However, the Owners will seek to ensure the request is legitimate.

13. Breaches

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