Curious Motion – Data Protection Policy

OVERVIEW

Curious Motion is committed to protecting the privacy of everyone involved in our work. This policy helps us to demonstrate how we seek to comply with data protection legislation and be accountable for our actions.

All members of staff (employed or freelance) and volunteers must comply with these procedures for processing or transmitting personal data.

It is our desire that employees, volunteers, and freelancers recognise the risks involved when dealing with such information and fully understand the steps that must be taken in order to minimise such risks. It is Curious Motion's policy to educate and inform employees, volunteers, and freelancers about the dangers of inappropriate and illegal use of the personal data they may have access to.

To help protect people's personal data all staff and volunteers should adhere to the following:

GENERAL

- Always treat people's personal information with integrity and confidentiality.
- Know what the data protection principles are and apply them.

DEVICES & ACCESS

- Make sure your devices (computer, mobile phone etc) are password protected.
- Passwords should be strong and changed regularly.
- If you access emails on your phone, this needs to have a security measure in place (e.g. face or touch ID).
- If possible, enable remote data wiping if your device is lost or stolen.
- Lock your phone when you aren't using it.
- Ensure your password is enabled/device is locked whenever you're away from your screen.
- Use your own device where you can, don't download or access sensitive data on other people's devices.
- Close down documents when you are not working on them.
- Use secure, not public wi-fi for all sensitive data.
- Be aware of where you are accessing sensitive data – for example, if you're in a public place can someone read your screen?
- Report losses of data or devices as soon as possible to Samantha McCormick.

COMMUNICATIONS

- Where applicable, use your Curious Motion email address for correspondence, rather than your personal email address.
- Be alert to cyber-attacks and report suspicious emails or calls.
- Take care to use the 'bcc' option for bulk emailing to ensure contact details are not shared.
- Beware of autocomplete on email. Check you are sending to the right address.
- If in doubt speak to Samantha McCormick first.

STORING/ DELETING DATA

Curious Motion – Data Protection Policy

- Any sensitive data that you have accessed and downloaded to your device should be fully deleted after use – make sure to empty your trash.
- Don't print documents unless absolutely necessary, and then cross-shred afterwards.

INTRODUCTION

The security and management of data is important to ensure that we can function effectively and successfully for the benefit of our participants, team and for the wider community.

It is essential that people's privacy is protected through the lawful and appropriate use and handling of their personal information, in line with the General Data Protection Regulation.

Every member of Curious Motion's team, including staff and volunteers has a responsibility to adhere to the Data Protection Principles outlined in the GDPR, and to this Data Protection Policy.

If you have a question about this Data Protection Policy or an area of concern about data protection matters, please contact our Data Protection Officer (DPO). The DPO is **Samantha McCormick.**

DATA PROTECTION PRINCIPLES

There are six Data Protection Principles defined in Article 5 of the GDPR. These require that all personal data be:

- processed in a **lawful**, **fair** and **transparent** manner.
- collected only for **specific**, **explicit** and **limited** purposes ('purpose limitation').
- **adequate**, **relevant** and **not excessive** ('data minimisation').
- **accurate** and kept **up-to-date** where necessary.
- kept for **no longer than necessary** ('retention').
- The Data Processing Register will be reviewed at least every 6 months by the Data Protection Officer with the involvement of the other necessary members of the team.
- handled with appropriate **security** and **confidentiality**.

We are committed to upholding the Data Protection Principles. All personal data under our control must be processed in accordance with these principles.

LAWFUL PROCESSING

All processing of personal data must meet one of the six lawful bases defined in Article 6(2) of the GDPR:

- Where we have the **consent** of the data subject
- Where it is in our **legitimate interests** and this is not overridden by the rights and freedoms of the data subject.
- Where necessary to meet a **legal obligation**.
- Where necessary to fulfil a **contract**, or pre-contractual obligations.
- Where we are protecting someone's **vital interests**.
- Where we are fulfilling a **public task,** or acting under official authority.

Curious Motion – Data Protection Policy

Any special category data (sensitive types of personal data as defined in Article 9(1) of the GDPR) must further be processed only in the line with one of the conditions specified in Article 9(2).

Where processing is based on consent, the data subject has the option to easily withdraw their consent.

Where electronic direct marketing communications are being sent, the recipient should have the option to opt-out in each communication sent, and this choice should be recognised and adhered to by us.

DATA MINIMISATION & CONTROL

Data collection processes will be regularly reviewed by the Board of Directors to ensure that personal data collected and processed is kept to a minimum.

We will keep the personal data that we collect, use and share to the minimum amount required to be adequate for its purpose.

Where we do not have a legal obligation to retain some personal data, we will consider whether there is a business need to hold it.

We will retain personal data only for as long as it is necessary to meet its purpose, usually during the time a person is involved in our activities, and for up to five years after that point.

In the case of sharing personal data with any third party, only the data that is necessary to fulfil the purpose of sharing will be disclosed.

Anonymisation and pseudonymisation of personal data stored or transferred should be considered where doing so is a possibility.

ACCOUNTABILITY

The 'Data Protection Officer' (DPO) has the specific responsibility of overseeing data protection and ensuring that we comply with the data protection principles and relevant legislation.

The DPO will ensure that our Data Protection processes are kept up to date and demonstrates how the data protection principles are adhered to by our activities. Individual members of staff and volunteers have a duty to contribute to ensure that the measures outlined in this policy are accurately reflected in our practice.

All employees, volunteers, consultants, partners or other parties who will be handling personal data on behalf of Curious Motion will be appropriately trained and supervised where necessary.

The collection, storage, use and sharing of personal data will be regularly reviewed by the Data Protection Officer, the Board of Directors, and any relevant business area.

We will adhere to relevant codes of conduct where they have been identified and discussed as appropriate.

Curious Motion – Data Protection Policy

Where there is likely to be a high risk to individuals rights and freedoms due to a processing activity, we will first undertake a Data Protection Impact Assessment (DPIA) and consult with the ICO prior to processing if necessary.

USE OF THIRD PARTY SERVICES

Curious Motion uses third party services to process some data, for example we use Bookwhen.com to manage our class bookings, and we store our data via Google Workspace (Drive, Mail, etc).

In all cases, Curious Motion must only appoint third party processors who can provide sufficient guarantees around compliance with the GDPR and that the rights of data subjects will be protected.

Where a processor can demonstrate that they adhere to approved codes of conduct or certification schemes, this should be taken into consideration for choice of supplier.

Where Curious Motion uses a processor, a written contract with compulsory terms as set out in Article 28 of the GDPR must be in place (plus any additional requirements that we determine). Processors can only act on the instruction of Curious Motion.

RIGHTS OF DATA SUBJECTS

Under data protection laws, data subjects have certain rights:

- **Right to be informed**. The right to be told how their personal data is used in clear and transparent language.
- **Right of access**. The right to know and have access to the personal data we hold about them.
- **Right to data portability**. The right to receive their data in a common and machine-readable electronic format.
- **Right to be forgotten**. The right to have their personal data erased.
- **Right to rectification**. The right to have their personal data corrected where it is inaccurate or incomplete.
- **Right to object**. The right to complain and to object to processing.
- **Right to purpose limitation**. The right to limit the extent of the processing of their personal data.
- **Rights related to automated decision-making and profiling**. The right not to be subject to decisions without human involvement.

We will uphold individuals' rights under data protection laws and allow them to exercise their rights over the personal data we hold about them. Privacy information will acknowledge these rights and explain how individuals can exercise them. Most rights are not absolute, and the individual will be able to exercise them depending on the circumstances, and exemptions may apply in some cases.

Any request in respect of these rights should preferably be made in writing to hello@curiousmotion.org.uk, but we will also accept verbal requests.

There is no fee for facilitating a request, unless it is 'manifestly unfounded or excessive', in which case administrative costs can be recovered.

Requests that are 'manifestly unfounded or excessive' can be refused.

Curious Motion – Data Protection Policy

We will take reasonable measures to require individuals to prove their identity where it is not obvious that they are the data subject.

We will respond to the request within one month from the date of request or being able to identify the person, unless it is particularly complex (in which case we will respond in no longer than 90 days).

The DPO will ensure that required actions are taken and that the appropriate response is facilitated within the deadline.

The DPO will draw up procedures for responding to requests where necessary, for example, for facilitating Subject Access Requests.

REPORTING OF BREACHES

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

All members of staff should be vigilant and able to identify a suspected personal data breach. A breach could include:

- loss or theft of devices or data, including information stored on USB drives or on paper.
- hacking or other forms of unauthorised access to a device, email account, or the network.
- disclosing personal data to the wrong person, through wrongly addressed emails, or bulk emails that inappropriately reveal all recipients email addresses.
- alteration or destruction of personal data without permission.

Where a member of staff discovers or suspects a personal data breach, this should be reported to the DPO as soon as possible.

Where there is a likely risk to individuals' rights and freedoms, the DPO will report the personal data breach to the ICO within 72 hours of the organisation being aware of the breach.

Where there is also a likely high risk to individuals' rights and freedoms, Curious Motion will inform those individuals without undue delay.

The DPO will keep a record of all personal data breaches reported and follow up with appropriate measures and improvements to reduce the risk of reoccurrence.

REVIEW

This policy is to be reviewed annually as a minimum.

Last review: March 2022