Happiness Outdoors Project

Data Protection Policy

Introduction and Scope

This policy outlines the Happiness Outdoors Project (HOP) commitment to data protection and compliance with the UK Data Protection Act 2018, UK General Data Protection Regulation (UK GDPR) and the Data Use and Access Act (DUAA) 2025. The purpose of this policy is to ensure that all personal data held by HOP is processed lawfully, fairly and transparently, and that the rights of data subjects are protected. This policy applies to all individuals working on behalf of HOP, including Directors, staff, and volunteers as well as all those who participate in HOP activities.

1. Data Protection Lead

HOP have a designated Data Protection Lead who will be responsible for overseeing data protection and leading on any incident investigation and reporting. The Data Protection Lead will also ensure that all staff and volunteers are provided with any induction, on the job or other training and made aware of their data protection responsibilities.

2. Data Protection

Data protection is the practice of safeguarding personal information by applying data protection principles and complying with the Data Protection Act. The Data Protection Act is a UK law that regulates the processing of personal data. The UK Information Commissioner's Office (ICO)[1] provides guidelines on data protection that HOP will follow.

UK GDPR: The UK General Data Protection Regulation, which outlines the rules for processing personal data in the UK.
Data Processor: An individual or organisation that processes personal data on behalf of a data controller.
Data Controller: An individual or organisation that determines how and why personal data is processed.
Joint Data Controller: Two or more controllers that jointly determine the purposes and means of processing the same personal data. They are not joint controllers if they are processing the same data for different purposes.
Data Subject: An individual whose personal data is being processed.
Processing: Any operation performed on personal data, including collection, storage, use, and disclosure.
Personal Data: Any information that can identify a living individual, such as name, address, or email address, photos or film.
Sensitive Personal Data: Personal data that requires extra protection, such as health information or ethnic origin.
Direct Marketing: Any communication aimed at promoting a product or service directly to an individual.
PECR: The Privacy and Electronic Communications Regulations, which govern electronic direct marketing.
Valid Consent: Consent given freely, specifically, and informed, and can be withdrawn at any time.

[1] https://ico.org.uk/

Legitimate Business Purpose: A lawful reason for processing personal data that is necessary for the legitimate interests of the data controller or a third party.

3. Data Protection Principles

HOP will endeavour, to its best ability, to work within the following data protection principles.

Data is processed lawfully, fairly and in a transparent manner.

- There are several grounds on which data may be collected, including consent.
- HOP is clear that the collection of data is legitimate and consent to hold an individual's data has been obtained, where appropriate.
- HOP is open and honest about how and why data is collected and individuals have a right to access their data.

Data is collected for specified, explicit and legitimate purposes and not used for any other purpose.

- HOP is clear on what data will be collected and the purpose for which it will be used.
- Only data that is needed will be collected.
- When data is collected for a specific purpose, it will not be used for any other purpose, without the consent of the person whose data it is.

Data is adequate, relevant and limited to what is necessary.

- HOP collect all the data needed to get the job done.
- HOP will not collect data that is not needed.

Data is accurate and, where necessary, kept up to date.

- HOP will ensure that data collected is accurate and will have processes and/or checks to ensure that data which needs to be kept up-to-date is, for example, beneficiary, staff or volunteer records.
- HOP will correct any mistakes promptly.

Data is kept for no longer than is necessary. HOP understands what data is needed to be retained, for how long and why.

- HOP hold data only for as long as needed.
- That includes both hard copy and electronic data.
- Some data must be kept for specific periods of time (e.g. accounting, accident and incident forms).
- HOP has an archive and review process that ensures data no longer needed is destroyed.

Data is processed to ensure appropriate security, not only to protect against unlawful use, but also loss or damage.

Data is held securely so that it can only be accessed by those who need to do so. For example, paper documents are locked away, access to online folders in shared drives is restricted to those who need it, IT systems are password protected, and/or sensitive documents that may be shared (e.g. payroll, photos) are password protected.

Data is kept safe. HOP's IT systems have adequate anti-virus and firewall protection that is up-to-date. Staff understand what they must and must not do to safeguard against cyber-attack, and that passwords must be strong and not written down or shared.

Data is recoverable. HOP have adequate data back-up and disaster recovery processes.

4. Individual Rights

HOP recognise that individuals' rights include the right to be informed; of access, to rectification, erasure, restrict processing, data portability and to object.

5. Use of Imagery/Video

All imagery or video are considered the personal data of those recognisable individuals within the image or video. As such, consent will be sought prior to obtaining or subsequent use of any imagery/video. Individuals under 13 years of age are not legally able to give consent and consent will be sought from parent/carers.

HOP undertakes to operate within partner schools' Data Protection and Safeguarding policies with respect to the taking and use of imagery/video of any individual taking part in HOP related activities.

Any use of images/video of children for internal purposes of school communications (e.g. school newsletters, websites, social media) will be guided by school Data Protection and Safeguarding policies and relevant parental/carer consent.

HOP in agreement with school partners will seek separate parental/carer consent for use of images/video of children for purposes of HOP or HOP donors printed or internet-based communications, fundraising or reporting.

Consent requests and privacy notices, or other information provided to parent/carers will be written and presented in a way that is understandable, fair and in-line with data protection principles outlined above (Section 4).

All images/video of children will only be taken using school camera/video equipment or a designated HOP digital camera. The designated HOP digital camera will only be removed from school with images for which full parental consent has been obtained. These images will be removed from the camera at the end of each day and transferred HOP IT system where they will be password protected. Their storage and use will be logged in HOP data retention schedule.

6. Data Breach

A breach is more than only losing personal data. It is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

HOP will investigate the circumstances of any loss or breach, to identify if any action needs to be taken. Action might include changes in procedures, where this will help to prevent a re-occurrence or disciplinary or other action, in the event of negligence.

HOP will notify the ICO within 72 hours, of a breach if it is likely to result in a risk to the rights and freedoms of individuals. If unaddressed such a breach is likely to have a significant detrimental effect on individuals. For example:

- Result in discrimination.
- Damage to reputation.
- Financial loss.
- Loss of confidentiality or any other significant economic or social disadvantage.

7. Other Policies

This Data Protection policy will be adhered to in relation to other policies such as, safeguarding policy, volunteer policy etc.

8. Fundraising

HOP will ensure that any fundraising complies with the Data Protection Act and ICO guidelines and also the Fundraising Regulator guidelines including, if applicable, direct marketing. HOP will respect the privacy and contact preferences of our donors.

9. Fundraising Preference Service

HOP will respect the privacy and contact preferences of any donors. HOP will respond promptly to requests to cease contacts or complaints and act to address their causes.

10. Data Retention

HOP's data will only be kept for as long as there is an administrative need to do so in order to enable HOP to carry out its business or support functions, or for as long as it is required to demonstrate compliance for audit purposes or to meet legislative requirements.

In general, records are kept for 6 years after the end of the accounting year to which they relate but HOP does not keep personal records any longer than necessary and certain records may be required to be retained for longer (e.g. incident and accident forms). Factors affecting retention periods include legal requirements, storage costs, historical value, industry standards, and archival needs.

Approval and Review

This policy will be reviewed by the Directors annually, as part of the financial planning cycle.

Version No	Approved By	Approval Date	Main Changes	Review Period
1.0	Directors	July 2024	Initial draft approved	Annually
2.0	Directors	September 2025	No major changes made	Annually