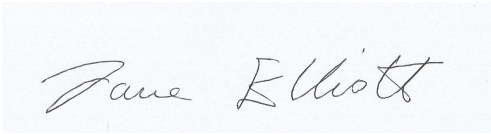




General Data Protection Regulation Policy (GDPR)

Formal Review Cycle:	Annual
Latest Formal Review Date (month/year):	01/2024
Next Formal Review Due (month/year):	01/2025
Approval Required - Trustees (Y/N):	
Signature 	
Date Approved:	04/01/2024
Publication:	Website

1. Introduction

Moor Time is committed to abiding by all applicable Data Protection laws and regulations and in line with the highest standards of ethical conduct. This policy sets forth the expected behaviours of Moor Time employees and third parties in relation to the collection, use, retention, transfer, disclosure and destruction of any personal data belonging to a Moor Time contact (i.e. the Data Subject).

Personal data is any information (including opinions and intentions) which relates to an identified or identifiable natural person. Personal data is subject to certain legal safeguards and other regulations, which impose restrictions on how organisations may process personal data. An organisation that handles personal data and makes decisions about its use is known as a

Data Controller. Moor Time, as a Data Controller, is responsible for ensuring compliance with the Data Protection requirements outlined in this policy. Non-compliance may expose Moor Time to complaints, regulatory action, fines and/or reputational damage.

Moor Times Senior Management Team is fully committed to ensuring continued and effective implementation of this policy, and expects all employees and third parties to share in this commitment. Any breach of this policy will be taken seriously and may result in disciplinary action or business sanction.

2. Scope

This policy applies to all Moor Time staff where a Data Subject's Personal Data is processed:

- In the context of the business activities of Moor Time
- For the provision or offer of goods or services to individuals (including those provided or offered free-of charge) by Moor Time.
- To actively monitor the behaviour of individuals.
- Monitoring the behaviour of individuals includes using data processing techniques such as persistent web browser cookies or dynamic IP address tracking to profile an individual with a view to:
 - Taking a decision about them.
 - Analysing or predicting their personal preferences, behaviours and attitudes.

This policy applies to all processing of personal data in electronic form (including electronic mail and documents created with word processing software) or where it is held in manual files that are structured in a way that allows ready access to information about individuals.

If there are any queries in regards to this policy, please consult with Moor Time Trustees for guidance using the following email address: hello@moortime.org.uk

3. Definitions

Employee	An individual who works for the Moor Time under a contract of employment, whether oral or written, express or implied, and has recognised rights and duties. Includes temporary employees and independent contractors.
Third Party	An external organisation with which Moor Time conducts business and is also

	authorised to, under the direct authority of Moor Time, Process the Personal Data of Moor Time Contacts.
Personal Data	Any information (including opinions and intentions) which relates to an identified or Identifiable Natural Person.
Contact	Any past, current or prospective Moor Time customer.
Identifiable Natural Person	Anyone who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
Data Controller	A natural or legal person, Public Authority, Agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.
Data Protection Officer (DPO) or Lead Person for Data Protection	A Data Protection Officer (DPO) is an enterprise security leadership role required by the General Data Protection Regulation (GDPR). Data Protection Officers are responsible for overseeing data protection strategy and implementation to ensure compliance with GDPR requirements
Data Subject	The identified or Identifiable Natural Person to which the data refers.
Process, Processed, Processing	Any operation or set of operations performed on Personal Data or on sets of Personal Data, whether or not by automated means. Operations performed may include collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Data Protection	The process of safeguarding Personal Data from unauthorised or unlawful disclosure,

	access, alteration, processing, transfer or destruction.
Data Protection Authority	An independent Public Authority responsible for monitoring the application of the relevant Data Protection regulation set forth in national law.
Data Processors	A natural or legal person, Public Authority, Agency or other body which Processes Personal Data on behalf of a Data Controller.
Consent	Any freely given, specific, informed and unambiguous indication of the Data Subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the Processing of Personal Data relating to him or her.
Special Categories of Data	Personal Data pertaining to or revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership; data concerning health or sex life and sexual orientation; genetic data or biometric data.
Third Country	Any country not recognised as having an adequate level of legal protection for the rights and freedoms of Data Subjects in relation to the Processing of Personal Data.
Profiling	Any form of automated processing of Personal Data where Personal Data is used to evaluate specific or general characteristics relating to an Identifiable Natural Person. In particular to analyse or predict certain aspects concerning that natural person's performance at work, economic situations, health, personal preferences, interests, reliability, behavior, location or movement.
Binding Corporate Rules	The Personal Data protection policies used for the transfer of Personal Data to one or more Third Countries within a group of undertakings, or group of enterprises engaged in a joint economic activity.
Personal Data Breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration,

	unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed.
Encryption	The process of converting information or data into code, to prevent unauthorised access.
Pseudonymisation	Data amended in such a way that no individuals can be identified from the data (whether directly or indirectly) without a "key" that allows the data to be re-identified.
Anonymisation	Data amended in such a way that no individuals can be identified from the data (whether directly or indirectly) by any means or by any person.

4. Policy

Lead Person for Data Protection

To demonstrate our commitment to Data Protection, and to enhance the effectiveness of our compliance efforts, Moor Time has established a lead person for data protection

Jane Elliott - Moor Time Trustee

Moortimejane@gmail.com

The Lead Person's duties include:

- Acting as a point of contact for and cooperating with Data Protection Authorities (DPAs- Information Commissioner's Office);
- Informing senior managers and trustees of any potential corporate, civil and criminal penalties which may be levied against Moor Time and/or its Employees for violation of applicable Data Protection laws.
- Ensuring establishment of procedures and standard contractual provisions for obtaining compliance with this Policy by any Third Party who:
 - provides Personal Data to Moor Time;
 - receives Personal Data from Moor Time;
 - has access to Personal Data collected or processed by Moor Time.
- Conduct an audit to identify what personal data is currently held, where it is stored, how it is used, and who it is shared with.

- The Lead Person will be available for receiving and processing of any GDPR complaints.
- Inform customers how Moor Time might share & use their personal data with a 3rd party. Provide 3rd party information & reason for sharing.
- Review and update procedures for handling subject access requests and also requests to correct or delete data that Moor Time holds.
- Ensuring all staff are aware of their specific role in making sure customer data is secure.

Policy Dissemination & Enforcement

The management team of Moor Time must ensure that all employees responsible for the Processing of Personal Data are aware of and comply with the contents of this policy. In addition, will make sure all Third Parties engaged to Process Personal Data on their behalf (i.e. their Data Processors) are aware of and comply with the contents of this policy. Assurance of such compliance must be obtained from all Third Parties, whether companies or individuals, prior to granting them access to Personal Data controlled by Moor Time.

Data Protection by Design

To ensure that all Data Protection requirements are identified and addressed when designing new systems or processes and/or when reviewing or expanding existing systems or processes.

Compliance Monitoring

To confirm that an adequate level of compliance is being achieved by all in relation to this policy, the Data Protection Lead will carry out an annual Data Protection compliance audit. Each audit will, as a minimum, assess: Compliance with Policy in relation to the protection of Personal Data, including:

- The assignment of responsibilities.
- Raising awareness.
- Review of Moor Times GDPR procedures

The lead will report the outcome of this exercise to the Trustees on an annual basis.

Data Protection Principles

All Moor Time employees are expected to abide by the Data Protection Principles as set out below:

Principle 1: Fairly and Lawfully - Personal data shall be processed fairly and lawfully. This means that Moor Time must have:

- legitimate grounds for collecting and using the personal data;
- not use the data in ways that have unjustified adverse effects on the individuals concerned;
- be transparent about how you intend to use the data, and give individuals appropriate privacy notices when collecting their personal data;
- handle people's personal data only in ways they would reasonably expect;

- and make sure you do not do anything unlawful with the data.

Principle 2: Purpose Limitation - Personal Data shall be collected for specified, explicit and legitimate purposes and not further Processed in a manner that is incompatible with those purposes. This means Moor Time must specify exactly what the Personal Data collected will be used for and limit the Processing of that Personal Data to only what is necessary to meet the specified purpose.

Principle 3: Data Minimisation - Personal Data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are Processed. This means Moor Time must not store any Personal Data beyond what is strictly required.

Principle 4: Accuracy - Personal Data shall be accurate and kept up to date. This means Moor Time must have in place processes for identifying and addressing out-of-date, incorrect and redundant Personal Data.

Principle 5: Storage Limitation - Personal Data shall be kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data is Processed. This means Moor Time must, wherever possible, store Personal Data in a way that limits or prevents identification of the Data Subject.

Principle 6: Integrity & Confidentiality - Personal Data shall be 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. Moor Time must use appropriate technical and organisational measures to ensure the integrity and confidentiality of Personal Data is maintained at all times.

Principle 7: Accountability - The Data Controller shall be responsible for, and be able to demonstrate compliance. This means Moor Time must demonstrate that the six Data Protection Principles (outlined above) are met for all Personal Data for which it is responsible.

Principle 8: International transfer - Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Data Collection

Data Sources

Personal Data should be collected only from the Data Subject unless one of the following apply:

- The nature of the business purpose necessitates collection of the Personal Data from other persons or bodies.
- The collection must be carried out under emergency circumstances in order to protect the vital interests of the Data Subject or to prevent serious loss or injury to another person.

If Personal Data is collected from someone other than the Data Subject, the Data Subject must be informed of the collection unless one of the following apply:

(A list of the disclosures that need to be made available to the Data Subject is provided in Appendix A)

- The Data Subject has received the required information by other means.
- The information must remain confidential due to a professional secrecy obligation.
- A national law expressly provides for the collection, Processing or transfer of the Personal Data.

Where it has been determined that notification to a Data Subject is required, notification should occur promptly, but in no case later than:

- One calendar month from the first collection or recording of the Personal Data.
- At the time of first communication if used for communication with the Data Subject.
- At the time of disclosure if disclosed to another recipient.

Data Subject Consent

Moor Time will obtain Personal Data only by lawful and fair means and, where appropriate with the knowledge and Consent of the individual concerned. Where a need exists to request and receive the Consent of an individual prior to the collection, use or disclosure of their Personal Data, Moor Time is committed to seeking such Consent.

The Data Protection Lead and other relevant representatives, shall establish a system for obtaining and documenting Data Subject Consent for the collection, processing, and/or transfer of their Personal Data.

The system must include provisions for:

- Determining what disclosures should be made in order to obtain valid Consent.
- Ensuring the request for consent is presented in a manner which is clearly distinguishable from any other matters, is made in an intelligible and easily accessible form, and uses clear and plain language.

- Ensuring the Consent is freely given (i.e. is not based on a contract that is conditional to the Processing of Personal Data that is unnecessary for the performance of that contract).
- Documenting the date, method and content of the disclosures made, as well as the validity, scope, and volition of the Consents given.
- Providing a simple method for a Data Subject to withdraw their Consent at any time.

Data Subject Notification

Moor Time will, when required by applicable law, contract, or where it considers that it is reasonably appropriate to do so, provide Data Subjects with information as to the purpose of the Processing of their Personal Data. When the Data Subject is asked to give Consent to the Processing of Personal Data and when any Personal Data is collected from the Data Subject, all appropriate disclosures will be made, in a manner that draws attention to them, unless one of the following apply:

- The Data Subject already has the information - must establish means for documenting the fact that the Data Subject already has the information and how it has been obtained.
- A legal exemption applies to the requirements for disclosure and/or Consent.

The disclosures may be given orally, electronically or in writing. If given orally, the person making the disclosures should use a suitable script or form approved in advance by the Data Protection Lead: The associated receipt or form should be retained, along with a record of the facts, date, content, and method of disclosure.

Data Use

Data Processing

Moor Time uses the Personal Data of its Contacts for the following broad purposes:

- The general running and business administration of Moor Time.
- To provide services to our customers/young people.
- The ongoing administration and management of customer services.
- To meet its external legal obligations.

The use of a Data Subject's information should always be considered from their perspective and whether the use will be within their expectations or if they are likely to object. However, it will not be within their reasonable expectations that Moor Time would then provide their details to third parties for marketing purposes.

Moor Time will process Personal Data in accordance with all applicable laws and applicable contractual obligations. More specifically, Moor Time will not Process Personal Data unless at least one of the following requirements are met:

- The Data Subject has given Consent to the Processing of their Personal Data for one or more specific purposes.
- Processing is necessary for the performance of a contract to which the Data Subject is party or in order to take steps at the request of the Data Subject prior to entering into a contract.
- Processing is necessary for compliance with a legal obligation to which the Data Controller is subject.
- Processing is necessary in order to protect the vital interests of the Data Subject or of another natural person.
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Data Controller.
- Processing is necessary for the purposes of the legitimate interests pursued by the Data Controller or by a Third Party (except where such interests are overridden by the interests or fundamental rights and freedoms of the Data Subject, in particular where the Data Subject is a child).

There are some circumstances in which Personal Data may be further processed for purposes that go beyond the original purpose for which the Personal Data was collected. When making a determination as to the compatibility of the new reason for Processing, guidance and approval must be obtained from the Data Protection Lead before any such Processing may commence.

In any circumstance where Consent has not been gained for the specific Processing in question, Moor Time will address the following additional conditions to determine the fairness and transparency of any Processing beyond the original purpose for which the Personal Data was collected:

- Any link between the purpose for which the Personal Data was collected and the reasons for intended further Processing.
- The context in which the Personal Data has been collected, in particular regarding the relationship between Data Subject and the Data Controller.
- The nature of the Personal Data, in particular whether Special Categories of Data are being Processed, or whether Personal Data related to criminal convictions and offences are being Processed.
- The possible consequences of the intended further Processing for the Data Subject.
- The existence of appropriate safeguards pertaining to further Processing, which may include Encryption, Anonymisation or Pseudonymisation.

Special Categories of Data

Moor Time will only Process Special Categories of Data (also known as sensitive data) where the Data Subject expressly consents to such Processing or where one of the following conditions apply:

- The Processing relates to Personal Data which has already been made public by the Data Subject.
- The Processing is necessary for the establishment, exercise or defence of legal claims.
- The Processing is specifically authorised or required by law.
- The Processing is necessary to protect the vital interests of the Data Subject or of another natural person where the Data Subject is physically or legally incapable of giving consent.
- Further conditions, including limitations, based upon national law related to the Processing of genetic data, biometric data or data concerning health.

In any situation where Special Categories Lead and the basis for the Processing clearly recorded with the Personal Data in question. Where Special Categories of Data are being Processed, Moor Time will adopt additional protection measures.

Moor Time may also adopt additional measures to address local custom or social expectation over the Processing of Special Categories of Data.

Children's Data

Children (*The age by which an individual is designated a child varies between 13 and 16 in accordance with national law.*) are unable to Consent to the Processing of Personal Data for information society services (*Any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services*). Consent must be sought from the person who holds parental responsibility over the child. However, it should be noted that where Processing is lawful under other grounds, Consent need not be obtained from the child or the holder of parental responsibility. Should Moor Time foresee a business need for obtaining parental consent for information society services offered directly to a child, guidance and approval must be obtained from the Data Protection Officer before any Processing of a child's Personal Data may commence.

Safeguarding

Moor Time will process data for safeguarding purposes lawfully and without consent where necessary for the purposes of: protecting an individual from neglect or physical and emotional harm; or. protecting the physical, mental or emotional wellbeing of an individual.

Data Quality

Moor Time will adopt all necessary measures to ensure that the Personal Data it collects and Processes is complete and accurate in the first instance, and is updated to reflect the current situation of the Data Subject.

The measures adopted to ensure data quality include:

- Correcting Personal Data known to be incorrect, inaccurate, incomplete, ambiguous, misleading or outdated, even if the Data Subject does not request rectification.
Correction may include data erase and replacement with corrected or supplemented data.
- Keeping Personal Data only for the period necessary to satisfy the permitted uses or applicable statutory retention period.
- The removal of Personal Data if in violation of any of the Data Protection principles or if the Personal Data is no longer required.
- Restriction, rather than deletion of Personal Data, insofar as:
 - a law prohibits erasure.
 - erasure would impair legitimate interests of the Data Subject.
 - the Data Subject disputes that their Personal Data is correct and it cannot be clearly ascertained whether their information is correct or incorrect.

Digital Marketing

As a general rule Moor Time will not send promotional or direct marketing material to a Contact through digital channels such as mobile phones, email and the Internet, without first obtaining their Consent. Any one wishing to carry out a digital marketing campaign without obtaining prior Consent from the Data Subject must first have it approved by the Data Protection Lead.

Where Personal Data Processing is approved for digital marketing purposes, the Data Subject must be informed at the point of first contact that they have the right to object, at any stage, to having their data Processed for such purposes.

If the Data Subject puts forward an objection, digital marketing related Processing of their Personal Data must cease immediately and their details should be kept on a suppression list with a record of their opt-out decision, rather than being completely deleted. It should be noted that where digital marketing is carried out in a 'business to business' context, there is no legal requirement to obtain an indication of Consent to carry out digital marketing to individuals provided that they are given the opportunity to opt-out.

Data Retention

To ensure fair Processing, Personal Data will not be retained by Moor Time for longer than necessary in relation to the purposes for which it was originally collected, or for which it was further Processed. The length of time for which we need to retain Personal Data is set out in the 'Document Retention Policy'.

This takes into account the legal and contractual requirements, both minimum and maximum, that influence the retention periods set forth in the schedule. All Personal Data should be deleted or destroyed as soon as possible where it has been confirmed that there is no longer a need to retain it.

Data Protection

Moor Time will adopt physical, technical, and organisational measures to ensure the security of Personal Data. This includes the prevention of loss or damage, unauthorised alteration, access or Processing, and other risks to which it may be exposed by virtue of human action or the physical or natural environment.

A summary of the Personal Data related security measures is provided below:

- Prevent unauthorised persons from gaining access to data processing systems in which Personal Data are processed.
- Prevent persons entitled to use a data processing system from accessing Personal Data beyond their needs and authorisations.
- Ensure that Personal Data in the course of electronic transmission during transport cannot be read, copied, modified or removed without authorisation.
- Ensure that in the case where Processing is carried out by a Data Processor, the data can be Processed only in accordance with the instructions of the Data Controller.
- Ensure that Personal Data is protected against undesired destruction or loss.
- Ensure that Personal Data collected for different purposes can and is Processed separately.
- Ensure that Personal Data is not kept longer than necessary.

Data Subject Requests

The Data Protection Lead will establish a system to enable and facilitate the exercise of Data Subject rights related to:

- Information access.
- Objection to Processing.
- Objection to automated decision-making and profiling.
- Restriction of Processing.
- Data portability.
- Data rectification.
- Data erasure.

If an individual makes a request relating to any of the rights listed above, Moor Time will consider each such request in accordance with all applicable Data Protection laws and

regulations. No administration fee will be charged for considering and/or complying with such a request unless the request is deemed to be unnecessary or excessive in nature.

Appendix C provides a standard form for the collection of information from the Data Subject by the DPO to progress the individual's request.

Data Subjects are entitled to obtain, based upon a request made in writing to the Data Protection Lead and upon successful verification of their identity, the following information about their own Personal Data:

- The purposes of the collection, Processing, use and storage of their Personal Data.
- The source(s) of the Personal Data, if it was not obtained from the Data Subject;
- The categories of Personal Data stored for the Data Subject.
- The recipients or categories of recipients to whom the Personal Data has been or may be transmitted, along with the location of those recipients.
- The envisaged period of storage for the Personal Data or the rationale for determining the storage period.
- The use of any automated decision-making, including Profiling.
- The right of the Data subject to:
 - object to Processing of their Personal Data.
 - lodge a complaint with the Data Protection Authority.
 - request rectification or erasure of their Personal Data.
 - request restriction of Processing of their Personal Data.

All requests received for access to or rectification of Personal Data must be directed to the Data Protection Lead, who will log each request as it is received.

A response to each request will be provided within 30 days of the receipt of the written request from the Data Subject. Appropriate verification must confirm that the requestor is the Data Subject or their authorised legal representative.

Data Subjects shall have the right to require Moor Time to correct or supplement erroneous, misleading, outdated, or incomplete Personal Data.

If Moor Time cannot respond fully to the request within 30 days, the Data Protection Lead shall nevertheless provide the following information to the Data Subject, or their authorised legal representative within the specified time:

- An acknowledgement of receipt of the request.
- Any information located to date.
- Details of any requested information or modifications which will not be provided to the Data Subject, the reason(s) for the refusal, and any procedures available for appealing the decision.
- An estimated date by which any remaining responses will be provided.

- An estimate of any costs to be paid by the Data Subject (e.g. where the request is excessive in nature).
- The name and contact information of the individual who the Data Subject should contact for follow up. It should be noted that situations may arise where providing the information requested by a Data Subject would disclose Personal Data about another individual. In such cases, information must be redacted or withheld as may be necessary or appropriate to protect that person's rights.

Law Enforcement Requests & Disclosures

In certain circumstances, it is permitted that Personal Data be shared without the knowledge or Consent of a Data Subject. This is the case where the disclosure of the Personal Data is necessary for any of the following purposes:

- The prevention or detection of crime.
- The apprehension or prosecution of offenders.
- The assessment or collection of a tax or duty.
- By the order of a court or by any rule of law.

If Moor Time Processes Personal Data for one of these purposes, then it may apply an exception to the Processing rules outlined in this policy but only to the extent that not doing so would be likely to prejudice the case in question.

If any employee receives a request from a court or any regulatory or law enforcement authority for information relating to Moor Time Contact, you must immediately notify the Data Protection Lead.

Data Protection Training

All employees that have access to Personal Data will have their responsibilities under this policy outlined to them as part of their staff induction training.

In addition, we will provide regular Data Protection training and procedural guidance for staff. The training and procedural guidance set forth will consist of, at a minimum, the following elements:

- The Data Protection Principles set forth in Section 4.2 above.
- Each Employee's duty to use and permit the use of Personal Data only by authorised persons and for authorised purposes.
- The need for, and proper use of, the forms and procedures adopted to implement this policy.
- The correct use of passwords, security tokens and other access mechanisms.
- The importance of limiting access to Personal Data, such as by using password protected screen savers and logging out when systems are not being attended by an authorised person.
- Securely storing manual files, print outs and electronic storage media.

- The need to obtain appropriate authorisation and utilise appropriate safeguards for all transfers of Personal Data outside of the internal network and physical office premises.
- Proper disposal of Personal Data by using secure shredding facilities.
- Any special risks associated with particular departmental activities or duties.

Complaints

Handling Data Subjects with a complaint about the Processing of their Personal Data, should put forward the matter in writing to the Data Protection Lead. An investigation of the complaint will be carried out to the extent that is appropriate based on the merits of the specific case. The Data Protection Lead will inform the Data Subject of the progress and the outcome of the complaint within a reasonable period. If the issue cannot be resolved through consultation between the Data Subject and the Data Protection Lead, then the Data Subject may, at their option, seek redress through mediation, binding arbitration, litigation, or via complaint to the Data Protection Authority within the applicable jurisdiction.

Breach Reporting

Any individual who suspects that a Personal Data Breach has occurred due to the theft or exposure of Personal Data must immediately notify the Data Protection Lead providing a description of what occurred. Notification of the incident can be made via e-mail at moortimejane@gmail.com. The Data Protection Lead will investigate all reported incidents to confirm whether or not a Personal Data Breach has occurred. If a Personal Data Breach is confirmed, the Data Protection Officer will follow the relevant authorised procedure based on the criticality and quantity of the Personal Data involved. For severe Personal Data Breaches, the SMT will initiate and chair an emergency response team to coordinate and manage the Personal Data Breach response.

All Data Breaches must be reported to the next scheduled annual report to the Trustees.

Appendix A - Information Notification to Data Subjects

The table below outlines the various information elements that must be provided by the Data Controller to the Data Subject depending upon whether or not Consent has not been obtained from the Data Subject.

Information Requiring Notification	With Consent	Without Consent
The identity and the contact details of the Data Controller and, where applicable, of the Data Controller's representative.	✓	✓

The original source of the Personal Data, and if applicable, whether it came from a publicly accessible source.		✓
The contact details of the Data Protection Officer, where applicable.	✓	✓
The purpose(s) and legal basis for Processing the Personal Data.	✓	✓
The categories of Personal Data concerned.	✓	✓
The recipients or categories of recipients of the Personal Data.	✓	✓
Where the Data Controller intends to further Process the Personal Data for a purpose other than that for which the Personal Data was originally collected, the Data Controller shall provide the Data Subject, prior to that further Processing, with information on that other purpose.	✓	✓
Where the Data Controller intends to transfer Personal Data to a recipient in a Third Country, notification of that intention and details regarding adequacy decisions taken in relation to the Third Country must be provided.	✓	✓
The period for which the Personal Data will be stored, or if that is not possible, the criteria used to determine that period.	✓	✓
Where applicable, the legitimate interests pursued by the Data Controller or by a Third Party.	✓	✓
The existence of Data Subject rights allowing them to request from the Data Controller-	✓	✓

information access, objection to Processing, objection to automated decision-making and profiling, restriction of Processing, data portability, data rectification and data erasure.		
Where Processing is based on Consent, the existence of the right to withdraw Consent at any time, without affecting the lawfulness of Processing based on Consent before its withdrawal.	✓	
The right to lodge a complaint with a Data Protection Authority.	✓	✓
The existence of automated decision-making (including Profiling) along with meaningful information about the logic involved and the significance of any envisaged consequences of such Processing for the Data Subject.	✓	✓
Whether the provision of Personal Data is a statutory or contractual requirement, a requirement necessary to enter into a contract, as well as whether the Data Subject is obliged to provide the Personal Data and if so the possible consequences of failure to provide such data.	✓	✓

Appendix B - Adequacy for Personal Data Transfers

The following are a list of countries recognised as having an adequate level of legal protection for the rights and freedoms of Data Subjects in relation to the Processing of their Personal Data. • EU Countries (Austria, Belgium, Bulgaria, Croatia, Republic of Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden and the UK) • Iceland • Liechtenstein • Norway • Andorra • Argentina • Canada (commercial organisations) • Faeroe Islands • Guernsey • Israel • Isle of Man • Jersey • New Zealand • Switzerland • Uruguay • United States (Privacy Shield certified organisations)

The following are a list of Third Country transfer mechanisms that can provide adequate protection when transfers are made to countries lacking an adequate level of legal protection. Appropriate safeguards

- Model Clauses
- Binding Corporate Rules
- Codes of Conduct
- Certification Mechanisms
- Derogations
- Explicit Consent
- Compelling Legitimate Interests
- Important reasons of Public Interest
- Transfers in response to a foreign legal requirement
- DPA approved contracts between Data Controllers and Data Processors

Appendix C - Standard Request Form for Access to Data

Data Access Request Form

Young people, parents/carers, staff and any other users of Moor Time have the right to access personal data relating to themselves that is held by Moor Time as part of a 'relevant filing system' (both in electronic and manual format).

Any individual who wishes to access data should apply using this Data Access Request Form.

1) ARE YOU THE DATA SUBJECT?

Yes – are you applying for data Moor Time holds about you? You will need to supply us with evidence of your identity (passport, proof of address, driving licence, birth certificate (or photocopy) etc.) as well as a signed copy of this form. This is to ensure we only release data to those who have a right to see the information.

Now complete Q2, 4 and 5

Are you acting on behalf of the Data Subject with their written authority? If so, you will need to enclose an original copy of their permission to disclose. This can be a letter which is signed personally by them giving you authority. We must be able to confirm from our records that this request relates to the Data Subject. You will be the applicant. The Data Subject details must be included at Q3.

Now complete Q 2, 3, 4 and 5

2) DETAILS OF APPLICANT

Surname: _____ First Names: _____

Former Surname (if applicable): _____

Address (Including postcode): _____

Telephone (day): _____ Telephone (eve): _____
Mobile: _____ Email: _____

3a) Details of the Data Subject (if different to 2)

Full Name: _____
Address: _____
Telephone Number: _____
Email: _____

3b) Please describe your relationship with the Data Subject that leads you to make this request on their behalf

_____ Complete 4 a/b/c as

appropriate

4a) CUSTOMER - Are you a present or past customer of Moor Time?

Yes/ No Present/Past

If yes, please give your dates of attendance: _____

4b) STAFF Are you a present or past member of staff?

Yes/ No Present/Past

4c) OTHERS - please provide details of your connection with the Holiday Club:

5) INFORMATION SOUGHT/ REQUIRED

Please be specific if there is particular information you require and identify where you think this information will be held:

Declaration

I....., certify that the information given on this application form to Moor Time is true. I understand that it is necessary for Moor Time to confirm my identity and it may be necessary to obtain more detailed information in order to locate the correct information.

Signed:

Date:

Please return the form to the Data Protection Lead, Moor Time, 9 Tivoli Place, Ilkley, West Yorkshire, LS29 8SU

Documents which must accompany this application are: 1. evidence of your identity 2. evidence of the Data Subject's identity (if different from above) 3. evidence of Data Subject's consent to disclose to a third party (if required as indicated above) 4. stamped addressed envelope for return of proof of identity/authority documents, where appropriate

Please note that Moor Time reserves the right to obscure or suppress information that relates to other third parties (as per the current Data Protection legislation)