Equal Opportunities for All Abilities and Empowering All Voices

Data Protection Policy

MOCHII

Approved by the Executive Committee: Sept 2024

Chair: Natalie Golawska

Review date: Sept 2025

DATA PROTECTION POLICY

Introduction

MOCHII is committed to being transparent about how it collects and uses the personal data of its workforce, and to meeting its data protection obligations. This policy sets out MOCHII's commitment to data protection, and individual rights and obligations in relation to personal data and demonstrates how MOCHII complies with the General Data Protection Regulation (GDPR) and Data Protection Act 2018.

This policy applies to the personal data of all working for MOCHII and any former employees, referred to as HR-related personal data. This policy does not apply to the personal data of clients or other personal data processed for business purposes.

MOCHII does not have a nominated Data Protection Officer, but if you have any queries concerning data protection you should speak to a member of management who will either be able to personally answer your query or direct this to an appropriate member of the management team who will be able to assist further.

Under the GDPR and Data Protection Act 2018, additional protections for job applicants, employees and other data subjects apply if an employer is processing "special categories" of personal data and criminal records data. One of these protections is a requirement to have an appropriate policy document in place. The relevant section of this policy sets out MOCHII's approach to processing special category personal data and criminal records data.

Data is grouped into three main areas and is defined as follows:

"Personal data" is any information that relates to a living individual who can be identified from that information. Processing is any use that is made of data, including collecting, storing, amending, disclosing or destroying it.

"Special categories of personal data" means information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and genetic and biometric data.

"Criminal records data" means information about an individual's criminal convictions and offences, and information relating to criminal allegations and proceedings.

MOCHII will keep all elements of this policy under review and if necessary, will make amendments as required to ensure that the policy remains up to date and accurately reflects MOCHII's approach to processing data.

Data protection principles

MOCHII processes HR-related personal data in accordance with the following data protection principles:

MOCHII processes personal data lawfully, fairly and in a transparent manner.

MOCHII collects personal data only for specified, explicit and legitimate purposes.

MOCHII processes personal data only where it is adequate, relevant and limited to what is necessary for the purposes of processing.

MOCHII keeps accurate personal data and takes all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay. MOCHII keeps personal data only for the period necessary for processing.

MOCHII adopts appropriate measures to make sure that personal data is secure, and protected against unauthorised or unlawful processing, and accidental loss, destruction or damage.

MOCHII tells individuals the reasons for processing their personal data, how it uses such data and the legal basis for processing in its privacy notices. It will not process personal data of individuals for other reasons. If MOCHII wants to start processing HR-related data for other reasons, individuals will be informed of this before any processing begins.

HR-related data will not be shared with third parties, except as set out in privacy notices. Where MOCHII relies on its legitimate interests as the basis for processing data, it will carry out an assessment to ensure that those interests are not overridden by the rights and freedoms of individuals.

Where MOCHII processes special categories of personal data or criminal records data to perform obligations, to exercise rights in employment law, or for reasons of substantial public interest, this is done in accordance with the relevant elements of this policy.

MOCHII will update HR-related personal data promptly if an individual advises that their information has changed or is inaccurate.

Personal data gathered during the working relationship is held in the individual's personnel file (in hard copy or electronic format, or both), and on HR systems. The periods for which MOCHII holds HR-related personal data are contained in its privacy notices to individuals.

MOCHII keeps a record of its processing activities in respect of HR-related personal data in accordance with the requirements of the GDPR and Data Protection Act 2018.

Individual rights

As a data subject, individuals have a number of rights in relation to their personal data.

Subject access requests

Individuals have the right to make a subject access request. If an individual makes a subject access request, MOCHII will tell them:

whether their data is processed and if so why, the categories of personal data concerned and the source of the data if it is not collected from the individual; to whom their data is or may be disclosed, including to recipients located outside the UK and the safeguards that apply to such transfers; for how long their personal data is stored (or how that period is decided); their rights to rectification or erasure of data, or to restrict or object to processing; their right to complain to the Information Commissioner if they think MOCHII has failed to comply with their data protection rights; and

whether MOCHII carries out automated decision-making and the logic involved in any such decision-making.

MOCHII will also provide the individual with a copy of the personal data undergoing processing. This will normally be in electronic form if the individual has made a request electronically, unless they agree otherwise.

To make a subject access request, the individual should send this via email/letter to the their line manager. In some cases, MOCHII may need to ask for proof of identification before the request can be processed. MOCHII will inform the individual if it needs to verify their identity and the documents it requires.

MOCHII will normally respond to a request within a period of one month from the date it is received. In some cases, such as where the request is complex, it may respond within three months of the date the request is received. MOCHII will write to the individual within one month of receiving the original request to tell them if this is the case.

If a subject access request is manifestly unfounded or excessive, MOCHII is not obliged to comply with it. Alternatively, MOCHII can agree to respond but will charge a fee, which will be based on the administrative cost of responding to the request. A subject access request is likely to be manifestly unfounded if it is made with the intention of harassing MOCHII or causing disruption, or excessive where it repeats a request to which MOCHII has already responded. If an individual submits a request that is unfounded or excessive, MOCHII will notify them that this is the case and whether it will respond to it.

Other rights

Individuals have a number of other rights in relation to their personal data. They can require MOCHII to: rectify inaccurate data;

stop processing or erase data that is no longer necessary for the purposes of processing;

stop processing or erase data if the individual's interests override MOCHII's legitimate grounds for processing data (where MOCHII relies on its legitimate interests as a reason for processing data); stop processing or erase data if processing is unlawful; and

stop processing data for a period if data is inaccurate or if there is a dispute about whether the individual's interests override MOCHII's legitimate grounds for processing data.

To ask MOCHII to take any of these steps, the individual should send the request to the management team at n.a.mochii@outlook.com

Data security

MOCHII takes the security of HR-related personal data seriously. MOCHII has internal policies and controls in place to protect personal data against loss, accidental destruction, misuse or disclosure, and to ensure that data is not accessed, except by employees in the proper performance of their duties.

Where MOCHII engages third parties to process personal data on its behalf, such parties do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

Impact assessments

There may be some instances where processing data that MOCHII carries out may result in risks to privacy. Where processing would result in a high risk to individual rights and freedoms, MOCHII will carry out a data protection impact assessment to determine the necessity and proportionality of processing. This will include

considering the purposes for which the activity is carried out, the risks for individuals and the measures that can be put in place to mitigate those risks. **Data breaches**

If MOCHII discovers that there has been a breach of HR-related personal data that poses a risk to the rights and freedoms of individuals, it will report it to the Information Commissioner as soon as possible and without unreasonable delay. MOCHII will record all data breaches regardless of their effect.

If the breach is likely to result in a high risk to the rights and freedoms of individuals, it will tell affected individuals that there has been a breach and provide them with information about its likely consequences and the mitigation measures it has taken.

International data transfers

MOCHII will not transfer HR-related personal data to countries outside the UK.

Individual responsibilities

Individuals are responsible for helping MOCHII keep their personal data up to date. Individuals should let MOCHII know if data provided to MOCHII changes, for example if an individual moves house or changes bank details.

Individuals may have access to the personal data of other individuals and any of our customers/clients etc in the course of their working relationship with us. Where this is the case, MOCHII relies on individuals to help meet its data protection obligations to staff and any relevant third party working with us, such as customers and clients.

Individuals who have access to personal data are required: to access only data that they have authority to access and only for authorised purposes; not to disclose data except to individuals (whether inside or outside MOCHII) who have appropriate authorisation;

to keep data secure (for example by complying with rules on access to premises, computer access, including password protection, and secure file storage and destruction);

not to remove personal data, or devices containing or that can be used to access personal data, from MOCHII's premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device;

not to store personal data on local drives or on personal devices that are used for work purposes; and to report data breaches of which they become aware to the management team immediately.

Failing to observe these requirements may amount to a disciplinary offence, which will be dealt with under MOCHII's disciplinary procedure. Significant or deliberate breaches of this policy, such as accessing employee or customer data without authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to dismissal without notice. **Training**

MOCHII will provide training to all individuals about their data protection responsibilities as part of the induction process.

Individuals whose roles require regular access to personal data, or who are responsible for implementing this policy or responding to subject access

requests under this policy, will receive additional training to help them understand their duties and how to comply with them.

Special category personal data and Criminal records data

MOCHII processes special category personal data and criminal records data for the following purposes.

Equal opportunities monitoring

Data related to racial and ethnic origin, religious and philosophical beliefs, health (including information on whether an individual has a disability) and sexual orientation are processed for equal opportunities monitoring purposes.

Processing is in MOCHII's legitimate interests. These interests are not outweighed by the interests of data subjects.

Processing is necessary for monitoring equality of opportunity or treatment, as permitted by the Data Protection Act 2018 (under para.8 of sch.1). **Health**

Data related to health (including information on whether an individual has a disability) is processed to: ensure that MOCHII is complying with its health and safety obligations; assess whether an employee is fit for work;

carry out appropriate capability procedures if an employee is not fit for work; ensure that an employee receives sick pay or other benefits to which they may be entitled; and

allow MOCHII to comply with its duties under the Equality Act 2010 for individuals with a disability.

Processing is necessary for:

compliance with legal obligations (e.g. assessing an employee's fitness for work, complying with health and safety obligations, carrying out capability procedures and complying with Equality Act 2010 duties).

the purposes of performing or exercising obligations or rights imposed by law in connection with employment under para.1 of sch.1 of the Data Protection Act 2018 the performance of a contract and/or complying with legal obligations (e.g. administering sick pay and other benefits).

the purposes of performing or exercising obligations or rights imposed by law in connection with employment under para.1 of sch.1 of the Data Protection Act 2018.

Racial or ethnic origin

Data related to data subjects' nationality is processed to ensure that MOCHII is complying with its obligations to check that they are entitled to work in the UK.

Processing is necessary for the purposes of performing or exercising obligations or rights imposed by law in connection with employment under para.1 of sch.1 of the Data Protection Act 2018.

Criminal records data

Criminal records data is processed as part of recruitment processes and, where necessary, in the course of employment to verify that candidates are suitable for employment or continued employment and to comply with legal and regulatory obligations to which MOCHII is subject.

Processing is necessary for:

Use where there is no legal obligation to carry out criminal records checks but MOCHII can demonstrate that there is a potential risk of unlawful behaviour if they employ someone with a criminal record.

for the prevention or detection of unlawful acts under para.10 of sch.1 of the Data Protection Act 2018.

Compliance with processing data

MOCHII processes HR-related special category personal data and criminal records data in accordance with the following data protection principles:

Lawful, fair and transparent processing

MOCHII processes personal data lawfully, fairly and in a transparent manner and for specified, explicit and legitimate purposes.

Employers can process special category personal data only if they have a legal basis for processing and, in addition, one of the specific processing conditions relating to special category personal data, or criminal records data, applies.

Where necessary, MOCHII has conducted a data impact assessment in relation to each processing operation to understand how processing may affect data subjects. The impact assessment balances the importance to MOCHII of the reasons for processing special category personal data and criminal records data with the possible adverse impact on data subjects (for example in relation to intrusion into an individual's private life and the impact on the duty of trust and confidence between employer and employee).

Any impact assessment has concluded in each case that processing is necessary and proportionate in light of the other safeguards in place and does not pose a high risk to individuals.

MOCHII explains to data subjects how special category personal data and criminal records data is used when it collects the data. This information is set out in MOCHII's privacy notices.

MOCHII does not use the data for any other purpose [and it reviews its processing and policies regularly to ensure that it is not using special category personal data or criminal records data for any other purpose]. MOCHII will not do anything unlawful with personal data.

Special category personal data and criminal records data are not disclosed to third parties, except in the context of seeking medical advice from MOCHII's chosen occupational health adviser or other medical advisers who are subject

to a professional duty of confidentiality or reporting suspected offences to the appropriate authorities. MOCHII complies with the Access to Medical Reports Act 1988 where relevant.

Adequate, relevant and limited processing

MOCHII collects and retains the minimum amount of information necessary to allow it to achieve the purposes outlined in this policy.

As far as possible, information required for equal opportunities monitoring purposes is kept in an anonymised form. Monitoring forms are kept under review to ensure that the information collected is accurate and not excessive.

As far as possible, MOCHII relies on health questionnaires, rather than medical testing, to obtain necessary information. Any medical testing that is carried out is relevant to the purpose for which it is undertaken and is focused on those performing high-risk roles.

Criminal records checks are carried out only for individuals undertaking roles where MOCHII is under a legal obligation [or regulatory requirement] to perform such checks or where this is necessary for the prevention or detection of unlawful acts.

All data is reviewed periodically, and any unnecessary data is deleted.

Accuracy of data held

MOCHII takes reasonable steps to ensure that the personal data that it holds is accurate.

Special category personal data and criminal records data is obtained: directly

from job applicants, employees and other data subjects; or

from external sources that MOCHII is entitled to assume will provide accurate information, such as the Disclosure and Barring Service in the case of criminal records data, or medical professionals in the case of health data.

MOCHII keeps a record of the source of all data it collects and data is reviewed periodically and checked for accuracy. Appropriate records are kept of amendments to data.

MOCHII will erase or rectify inaccurate data that it holds without delay in accordance with this policy. If an individual notifies it that their personal data has changed or is otherwise inaccurate, or if it is otherwise found to be inaccurate. Individuals are reminded to review their data on a regular basis to ensure that it remains up to date. **Data retention**

MOCHII keeps personal data only for the period necessary for processing.

MOCHII has considered how long it needs to retain special category personal data and criminal records data. The periods for which special category personal data is retained after the end of employment are as follows:

Equal opportunities data is kept for a period of six months, after which data is anonymised so that individuals can no longer be identified. Racial or ethnic origin data is kept for a period of three years.

Health data is normally kept for a period of seven years] unless statutory requirements mean that MOCHII must keep records for longer than that.

MOCHII does not retain details of an individual's criminal record after the commencement of employment, although it will retain a note on individual HR files indicating that a satisfactory criminal records check was completed prior to the commencement of employment. The note will be deleted at the end of the employment.

At the end of the relevant retention period, MOCHII erases or securely destroys special category personal data and criminal records data.

This policy will be retained by MOCHII while special category personal data and criminal records data is being processed and for a period of at least six months after MOCHII stops carrying out such processing. **Security of data**

MOCHII takes the security of special category personal data and criminal records data seriously. MOCHII has internal policies and controls in place to protect personal data against loss, accidental destruction, misuse or disclosure, and to ensure that data is not accessed, except by employees in the proper performance of their duties. MOCHII has analysed the risk presented by processing special category personal data and criminal records data and taken this into account in assessing appropriate security requirements.