



# GDPR AND DATA PROTECTION POLICY

MIDLANDS ACADEMY OF DANCE AND DRAMA

VERSION 1.0



## GDPR and Data Protection Policy

---

### Contents

Version Control .....	3
Introduction .....	4
Scope.....	4
Definitions.....	5
Data Protection Principles.....	8
The Basis for Processing Personal Information.....	8
Sensitive Personal Information .....	9
Criminal Records Information - Staff.....	12
Data Protection Impact Assessments (DPIAs).....	12
Documentation and Records.....	13
General Controls in Place .....	14
Privacy Notice.....	14
Individual Rights .....	15
Individual Obligations.....	16
Information Security .....	17
Storage and Retention of Personal Information – Service users and Staff .....	18
Data Breaches .....	19
International Transfer of Data .....	20
Consequences of Failing to Comply .....	20
Data Storage and Retention.....	21
Systems Used and Data Stored .....	21
Sharing of Data – Service Users/Staff .....	21
Staff Data Stored.....	22
Service User Data Stored .....	24
Data Sharing Process Flow .....	26
Subject Access Requests and Data Rights – Service users and Staff .....	27



## GDPR and Data Protection Policy

---

Introduction.....	27
SAR and Data Rights Procedure .....	27
SAR Timescales.....	27
SAR Fees .....	27
SAR Business Processes.....	27
Undertaking Privacy Impact Assessments .....	28
Confidentiality.....	29
Service Users.....	29
Discussions and Meetings .....	30
Outside of Work .....	30
Requests for Information .....	30
Security of Personal Data .....	30
Disclosure Policy.....	31
Procedure on Disclosures.....	31
Staff Records .....	32
Outside of Work .....	32
Personal and Sensitive Information .....	32
Requests for Information .....	33
Disclosure Policy and Procedures .....	33
Procedure on Disclosures.....	33
Governance.....	33
Monitoring and Reviewing.....	33



## GDPR and Data Protection Policy

---

### Version Control

VERSION	REVIEWER NAME	DATE	NEXT REVIEW	COMMENTS
1.0		Nov 2022	Nov 2023	First Policy



## GDPR and Data Protection Policy

---

### Introduction

Midlands Academy of Dance & Drama (MADD) was founded in 1967 by the principal, Frances Clayton and is based in Nottingham. MADD offers diplomas in Professional Dance, Musical Theatre, classes to 3-18-year-olds, and qualifications in Teacher Training in Dance with the International Dance Teachers Association (IDTA).

This policy sets out how we comply with our data protection obligations and seek to protect personal information relating to individuals. Its purpose is also to ensure that Staff understands and comply with the rules governing the collection, use and deletion of personal information to which they may have access in the course of their work.

We are committed to complying with our data protection obligations, to being concise, clear, and transparent about how we obtain and use personal information relating to individuals and how and when we delete that information once it is no longer required.

The Scheduling, Policy & Compliance Officer is responsible for informing and advising MADD and its Staff on its data protection obligations and for monitoring compliance with those obligations and with other MADD policies.

If you have any questions or comments about the content of this policy or if you need further information, you should contact the data protection officer by emailing: [louise@maddcollege.co.uk](mailto:louise@maddcollege.co.uk) or by letter to MADD, Century House, Building B, 428 Carlton Hill, Nottingham, NG4 1HQ.

### Scope

This policy applies to all MADD staff.

This document is also applicable to other stakeholders in MADD.

MADD policy and procedure documents may be distributed to suppliers, accreditation, compliance bodies and any other relevant third parties.

In some cases, third parties, such as suppliers or those performing on-site work or through our online presence for MADD, will be expected to adhere to our policies, which will be made available where applicable.

We will review and update this policy adhering to our data protection obligations. It does not form part of any employee's contract of employment, and we may amend, update, or supplement it from time to time.



## GDPR and Data Protection Policy

---

We will circulate any new or modified policy to Staff and any other stakeholders when it is adopted.

### Definitions

<b>Criminal Records Information</b>	Personal information relating to criminal convictions and offences, allegations, proceedings, and related security measures.
<b>Data Breach</b>	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal information.
<b>Data Subject</b>	Means the individual to whom the personal information relates.
<b>Personal Information</b>	(Sometimes known as personal data) means information relating to an individual who can be identified (directly or indirectly) from that information.
<b>Processing Information</b>	Obtaining, recording, organising, storing, amending, retrieving, disclosing and/or destroying information, or using or doing anything with it.
<b>Pseudonymised</b>	Means the process by which personal information is processed in such a way that it cannot be used to identify an individual without the use of additional information which is kept separately and subject to technical and organisational measures to ensure that



## GDPR and Data Protection Policy

---

the personal information cannot be attributed to an identifiable individual.

**Sensitive Personal Information** Sometimes known as ‘special categories of personal data’ or ‘sensitive personal data’ means personal information about an individual’s race, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership (or non-membership), genetics information, biometric information (where used to identify an individual) and information concerning an individual’s health, sex life or sexual orientation.

**Processor** The UK GDPR defines a processor as a natural or legal person, public authority, agency, or other body which processes personal data on behalf of the controller. Processors act on behalf of the relevant controller and under their authority.

**Controller** Art.2(d) GDPR  
The natural or legal person, public authority, agency, or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by EU or Member State laws, the controller may be designated by those laws.



## GDPR and Data Protection Policy

---





## GDPR and Data Protection Policy

---

### Data Protection Principles

MADD will comply with the following data protection principles when processing personal information:

- We will process personal information lawfully, fairly and in a transparent manner.
- We will collect personal information for specified, explicit and legitimate purposes only, and will not process it in a way that is incompatible with those legitimate purposes.
- We will only process the personal information that is adequate, relevant, and necessary for the relevant purposes.
- We will keep accurate and up-to-date personal information and take reasonable steps to ensure that inaccurate personal information is deleted or corrected without delay.
- We will keep personal information for no longer than is necessary for the purposes for which the information is processed.
- We will take appropriate technical and organisational measures to ensure that personal information is kept secure and protected against unauthorised or unlawful processing, accidental loss, destruction, or damage.

### The Basis for Processing Personal Information

Concerning any processing activity, we will, before the processing starts for the first time and then regularly while it continues:

- Review the purposes of the processing activity, and select the most appropriate lawful basis (or bases) for that processing, for example:
  - That the data subject has consented to the processing.
  - That the processing is necessary for the performance of a contract to which the data subject is a party, or to take steps at the request of the data subject before entering into a contract.
  - That the processing is necessary for compliance with a legal obligation to which MADD is subject.
  - That the processing is necessary for the protection of the vital interests of the data subject or another natural person; or

## GDPR and Data Protection Policy

---

- That the processing is necessary for the performance of a task carried out in the public interest or exercise of official authority; or
  - That the processing is necessary for legitimate interests of MADD or a third party, except where those interests are overridden by the interests of fundamental rights and freedoms of the data subject.
- Except where the processing is based on consent, satisfy ourselves that the processing is necessary for the relevant lawful basis (for example, that there is no other reasonable way to achieve that purpose).
- Document our decision as to which lawful basis applies, to help demonstrate our compliance with the data protection principles.
- Include information about both the purposes of the processing and the lawful basis for it in our relevant privacy notice(s).
- Where sensitive personal information is processed, also identify a lawful special condition for processing that information and document it; and
- Where criminal offence information is processed, also identify a lawful condition for processing that information and document it.
- To determine whether MADD legitimate interests are the most appropriate basis for lawful processing, we will:
  - Conduct a legitimate interests assessment (LIA) and keep a record of it to ensure that we can justify our decision;
  - If the LIA identifies a significant privacy impact, consider whether we also need to conduct a data protection impact assessment (DPIA);
  - Keep the LIA under review and repeat it if circumstances change; and
  - Include information about our legitimate interests in our relevant privacy notice(s).

## Sensitive Personal Information



## GDPR and Data Protection Policy

---

Sensitive personal information is sometimes referred to as 'special categories of personal data' or 'sensitive personal data'.

- MADD may need to process sensitive personal information. We will only process sensitive personal information if:
  - We have a lawful basis for doing to set out as above, for example, it is necessary for the performance of the employment contract, to comply with our legal obligations to people or for legitimate interests; and
  - One of the special conditions for processing sensitive personal information applies, for example:
    - The data subject has given explicit consent so MADD can provide its services.
    - The processing is necessary for exercising the employment law rights or obligations of MADD or the data subject.
    - The processing is necessary to protect the data subject's vital interests and the data subject is physically incapable of giving consent.
    - Processing relates to personal data which is manifestly made public by the data subject.
    - The processing is necessary for the establishment, exercise, or defence of legal claims; or
    - The processing is necessary for reasons of substantial public interest.
- Before processing any sensitive personal information, Staff must inform the Data Protection Officer of the proposed processing so that the DPO may assess whether the processing complies with the criteria noted above.
- Sensitive personal information will not be processed until:
  - The assessment/training has been agreed to; and
  - The individual has been properly informed (by way of a privacy notice or otherwise) as to the nature of the processing, the purposes for which it is

## GDPR and Data Protection Policy

---

being carried out and the legal basis for it.

- MADD will not carry out automated decision-making (including profiling) based on an individual's sensitive personal information.
- MADD Privacy Notice sets out the types of sensitive personal information that MADD processes, what it is used for and the lawful basis for the processing.
- Concerning sensitive personal information, MADD will comply with the procedures set out to make sure that it complies with the data protection principles as set out above.
- During the recruitment process the organisation will ensure that (except where the law permits otherwise):
  - During the short-listing, interview and decision-making stages, no questions are asked relating to sensitive personal information, for example, race, ethnic origin, trade union membership or health.
  - If sensitive personal information is received, for example, the applicant provides it without being asked for it within their CV or during the interview, no record is kept of it and any reference to it is immediately deleted or redacted.
  - Any completed equal opportunities monitoring form is kept separate from the individual's application form, and not be seen by the person shortlisting, interviewing, or making the recruitment decision.
  - 'Right to work' checks are carried out before an offer of employment is made unconditional, and not during the earlier short-listing, interview, or decision-making stages.
  - We will not ask health questions in connection with recruitment.
- During the employment the organisation will process:
  - Health information to administer sick pay, keep sickness absence records, monitor staff attendance, and facilitate employment-related health and sickness benefits;



## GDPR and Data Protection Policy

---

- Sensitive personal information for equal opportunities monitoring and pay equality reporting, where possible, this information will be anonymised; and
- Trade union membership information for staff administration and administering 'check off'.

### Criminal Records Information - Staff

Any criminal records information will be processed following the Disclosure and Barring Service (DBS) best practices.

### Data Protection Impact Assessments (DPIAs)

Where the processing is likely to result in a high risk to an individual's data protection rights we will, before commencing the processing, carry out a DPIA to assess:

- Whether the processing is necessary and proportionate concerning its purpose.
- The risks to individuals.
- What measures can be put in place to address those risks and protect personal information.
- Before any new form of technology is introduced, the manager responsible should therefore contact the data protection officer so that a DPIA can be carried out.
- During any DPIA, the employer will seek the advice of the data protection officer and any other relevant stakeholders.



## GDPR and Data Protection Policy

---

### Documentation and Records

We will keep records of processing activities, including:

- The name and details of the individual;
- The purposes of the processing;
- A description of the categories of individuals and categories of personal data;
- Categories of recipients of personal data;
- Where relevant, details of transfers to third countries including documentation of the transfer mechanism safeguards in place;
- Where possible, retention schedules; and
- Where possible, a description of technical and organisational security measures.

As part of our record of processing activities we document, or link to documentation, on:

- Information required for privacy notices.
- Records of consent.
- Controller-processor contracts.
- The location of personal information.
- Data Protection Impact Assessments (DPIA).
- Records of data breaches.
- If we process sensitive personal information or criminal records information, we will keep written records of:
  - o The relevant purpose(s) for which the processing takes place, including (where required) why it is necessary for that purpose;
  - o The lawful basis for our processing;



## GDPR and Data Protection Policy

---

- o Whether we retain and/or erase the personal information following our policy document and, if not, the reasons for not following our policy.
- We will conduct regular reviews of the personal information we process and update our documentation accordingly. This may include:
  - o Carrying out information audits to find out what personal information MADD holds.
  - o Distributing questionnaires and talking to Staff across MADD to get a more complete picture of our processing activities; and
  - o Reviewing our policies, procedures, contracts, and agreements to address areas such as retention, security, and data sharing.
- We document our processing activities in electronic form so we can add, remove, and amend information easily.

### General Controls in Place

- There is a process of continual review to determine whether any changes in the organisation's registration are required because of changes in the nature of the charity.
- The details of MADD are registered are kept up to date.
- The notification to the Information Commissioner's Office has been renewed annually.
- MADD maintains and updates the public data protection register which will be reviewed regularly and at least on an annual basis.

### Privacy Notice

MADD will issue privacy notices from time to time, informing individuals about the personal information that we collect and hold relating to them, how they can expect their personal information to be used and for what purposes.

We will take appropriate measures to provide information in privacy notices in a concise, transparent, intelligible, and easily accessible form, using clear and plain language.



## GDPR and Data Protection Policy

---

### Individual Rights

People have the following rights concerning their personal information:

- To be informed about how, why and on what basis that information is processed.
- To obtain confirmation that that information is being processed and to obtain access to it and certain other information by making a subject access request— see the SAR Policy information.
- To have data corrected if it is inaccurate or incomplete.
- To have data erased if it is no longer necessary for the purpose for which it was originally collected/processed, or if there are no overriding legitimate grounds for the processing (this is sometimes known as ‘the right to be forgotten’).
- To restrict the processing of personal information where the accuracy of the information is contested, or the processing is unlawful (but an individual does not want the data to be erased), or where the employer no longer needs the personal information but requires the data to establish, exercise or defend a legal claim.
- To restrict the processing of personal information temporarily where they do not think it is accurate (and the controller is verifying whether it is accurate), or where an individual has objected to the processing (and the controller is considering whether the organisation’s legitimate grounds override their interests).
- If you wish to exercise any of the rights in the paragraphs above, please contact the data protection officer.





## GDPR and Data Protection Policy

---

### Individual Obligations

Individuals are responsible for helping MADD keep their personal information up to date. You should let MADD know if the information you have provided to MADD changes, for example, if you move to a new house or change details of the bank or building society account into which you are paid.

An individual may have access to the personal information of other members of Staff, suppliers, and service users of MADD in the course of their employment or engagement.

If so, MADD expects them to help meet its data protection obligations to those individuals. Staff should be aware that they may also enjoy the rights set out above.

If you have access to personal information, you must:

- Only access the personal information that you have the authority to access and only for authorised purposes.
- Only allow other organisational staff to access personal information if they have appropriate authorisation.
- Only allow individuals who are not organisational staff to access personal information if you have specific authority to do so from the data protection officer.
- Keep personal information secure by complying with rules on access to premises, computer access, password protection and secure file storage/ destruction and other precautions set out in this document.
- Not remove personal information or devices containing personal information (or which can be used to access it) from MADD premises unless appropriate security measures are in place (such as pseudonymisation, encryption or password protection).
- Not store personal information on local drives or on personal devices that are used for work purposes.
- You should contact the data protection officer if you are concerned or suspect that one of the following has taken place (or is taking place or is likely to take

## GDPR and Data Protection Policy

---

place):

- Processing of personal data without a lawful basis for its processing or, in the case of sensitive personal information, without one of the conditions being met;
- Any data breach as set out below;
- Access to personal information without the proper authorisation;
- Personal information not kept or deleted securely;
- Removal of personal information or devices containing personal information (or which can be used to access it) from MADD premises without appropriate security measures being in place;
- Any other breach of this Policy or any of the data protection principles set out above.

### Information Security

MADD will use appropriate technical and organisational measures to keep personal information secure and to protect against unauthorised or unlawful processing and accidental loss, destruction, or damage. These may include:

- Ensuring that, where possible, personal information is pseudonymised or encrypted;
- Ensuring the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- Ensuring that in the event of a physical or technical incident availability and access to personal information can be restored promptly;
- A process for regularly testing, assessing, and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.
- In rare cases where MADD uses external organisations to process personal information on its behalf, additional security arrangements need to be

## GDPR and Data Protection Policy

---

implemented in contracts with those organisations to safeguard the security of personal information. In particular, contracts with external organisations must state that:

- The organisation may act only on the written instructions of MADD;
  - Those processing the data are subject to a duty of confidence;
  - Appropriate measures are taken to ensure the security of processing;
  - Sub-contractors are only engaged with the prior consent of MADD and under a written contract;
  - The organisation will assist MADD in providing subject access and allowing individuals to exercise their rights under the GDPR;
  - The organisation will assist MADD in meeting its GDPR obligations concerning the security of processing, the notification of data breaches and data protection impact assessments;
  - The organisation will delete or return all personal information to MADD as requested at the end of the contract; and
  - MADD will submit to audits and inspections and provide MADD with whatever information it needs to ensure that they are both meeting their data protection obligations, and tell MADD immediately if it is asked to do something infringing data protection law.
- Before any new agreement involving the processing of personal information by an external organisation is entered into, or an existing agreement is altered, the relevant Staff must seek approval of its terms by the DPO.

### Storage and Retention of Personal Information – Service users and Staff

- Personal information and sensitive personal information will be kept securely.

Personal information and sensitive personal information should not be retained any longer than necessary. The length of time over which data should be kept will depend upon the circumstances, including the reasons why the personal information was obtained. Staff should



## GDPR and Data Protection Policy

---

follow MADD retention criteria defined in this document. Where there is any uncertainty, Staff should consult the data protection officer at [louise@maddcollege.co.uk](mailto:louise@maddcollege.co.uk)

- Personal information (and sensitive personal information) that is no longer required will be deleted permanently from our information systems and any hard copies will be destroyed securely.

### Data Breaches

- A data breach may take many different forms, for example:
  - Loss or theft of data or equipment on which personal information is stored;
  - Unauthorised access to or use of personal information either by a member of Staff or a third party;
  - Loss of data resulting from an equipment or systems (including hardware and software) failure;
  - Human error, such as accidental deletion or alteration of data;
  - Unforeseen circumstances, such as a fire or flood;
  - Deliberate attacks on IT systems, such as hacking, viruses, or phishing scams;
  - 'Blagging' offences, where information is obtained by deceiving the organisation which holds it.
- In the event of a Data Breach, MADD will:
  - Make the required report of a data breach to the Information Commissioner's Office without undue delay and, where possible, within 72 hours of becoming aware of it if it is likely to result in a risk to the rights and freedoms of individuals.
  - Notify the affected individuals if a data breach is likely to result in a high risk to their rights and freedoms and notification is required by law.
  - Risk assess the situation and determines what steps need to be taken.



## GDPR and Data Protection Policy

---

- Immediately take such steps as are necessary to minimise the risk to service users, Staff, and the organisation.
- Take such steps as are necessary to ensure that similar breaches cannot happen again.

### International Transfer of Data

MADD does not intend to transfer personal information outside the European Economic Area (EEA) (which comprises the countries in the European Union and Iceland, Liechtenstein, and Norway).

If this were to be required, it would be on the basis that that country, territory or organisation is designated as having an adequate level of protection OR that the organisation receiving the information has provided adequate safeguards by way of standard data protection clauses.

### Consequences of Failing to Comply

MADD takes compliance with this policy very seriously. Failure to comply with the policy:

- Puts at risk the individuals whose personal information is being processed; and
- Carries the risk of significant civil and criminal sanctions for the individual and MADD; and
- May, in some circumstances, amount to a criminal offence by the individual.

Because of the importance of this policy, a staff member's failure to comply with any requirement of it may lead to disciplinary action under our procedures and this action may result in dismissal for gross misconduct. If a non-employee breaches this policy, they may have their contract terminated with immediate effect.

If you have any questions or concerns about anything in this policy do not hesitate to contact the Data Protection Officer.



## GDPR and Data Protection Policy

---

### Data Storage and Retention

MADD stores limited personal and sensitive personal information on Staff and service users/service providers to manage and fulfil our day-to-day organisational requirements.

As we generally provide a matching service for service users to courses and the management of these courses, this information is limited in scope.

### Systems Used and Data Stored

All digital data is secured using the following systems on MADD-provisioned Laptops and Desktops:

- Office 365 programs.

Contractual information and CV's, as well as other relevant data, may be stored in digital formats and hard copies.

Any hard copies are stored in lockable filing cabinets in locked, secure rooms.

Access is only provisioned to the MADD staff members who have requirements to view and manage service user/service provider and staff data.

### Sharing of Data – Service Users/Staff

Staff/Service User data is only shared with the following individuals and organisations:

- Welfare organisations (if required).
- Police and Government related organisations (if required).
- Travel and Accommodation arrangements.
- Access to Venues.
- Payroll (Wilford Smith Associates).

## Staff Data Stored

Information Type
Staff Data
Data Stored
<p>Typical staff data stored. MADD may store parts or all the data depending on the individual use case and if they are a full-time staff member, part-time staff member, or subcontractor.</p> <p><b>Personal Information</b></p> <ul style="list-style-type: none"> <li>• Name, address, email, telephone number.</li> <li>• Next of Kin.</li> <li>• Application Form data/CV.</li> <li>• Interview notes.</li> <li>• Offer and acceptance letters.</li> <li>• Subcontractor Contracts.</li> </ul> <p><b>Contract</b></p> <ul style="list-style-type: none"> <li>• Dated/signed.</li> <li>• P60/P45.</li> </ul> <p><b>Photographic Evidence of Identity</b></p> <ul style="list-style-type: none"> <li>• Valid Passport/Driving Licence copy.</li> </ul> <p><b>Various</b></p> <ul style="list-style-type: none"> <li>• National Insurance and Bank details.</li> <li>• Copies of relevant qualifications.</li> <li>• Right to Work in the UK.</li> <li>• Evidence of Current Address.</li> <li>• References.</li> <li>• Training Record.</li> </ul>

## GDPR and Data Protection Policy

<ul style="list-style-type: none"> <li>• Record of sickness, leave and disciplinaries.</li> <li>• Statutory Maternity, Adoption, Paternity Pay, etc.</li> <li>• Statutory Sick Pay.</li> <li>• Payroll and PAYE Records.</li> <li>• Health and Safety Consultations.</li> <li>• DBS Check Data.</li> <li>• Redundancy Details.</li> <li>• Disciplinary, working time and training data.</li> <li>• Images and recordings.</li> </ul>
Processing Reason
<ul style="list-style-type: none"> <li>• Provision of employment obligations.</li> <li>• Fulfilment of contract.</li> </ul>
Legal Interest/Legitimate Reason
<ul style="list-style-type: none"> <li>• Legitimate reason for performing contract duties.</li> <li>• Consent is given by an individual at the initial stage (contract).</li> </ul>
Retention Policy
3 years.



## Service User Data Stored

<b>Information Type</b>
Service User Data
<b>Data Stored</b>
<p>Service User's Data may include:</p> <ul style="list-style-type: none"> <li>• Service users' names and contact information (address, email, phone number).</li> <li>• Medical and Dietary Requirements as well as allergies.</li> <li>• Course details and scheduling.</li> <li>• The parent/guardian of the service user's names and contact details, if relevant.</li> </ul>
<b>Processing Reason</b>
<ul style="list-style-type: none"> <li>• Administration of MADD services.</li> </ul>
<b>Legal Interest/Legitimate Reason</b>
<ul style="list-style-type: none"> <li>• Legitimate reason for performing contract duties.</li> <li>• Consent is given at the initial opt-in.</li> </ul>
<b>Retention Policy</b>



## GDPR and Data Protection Policy

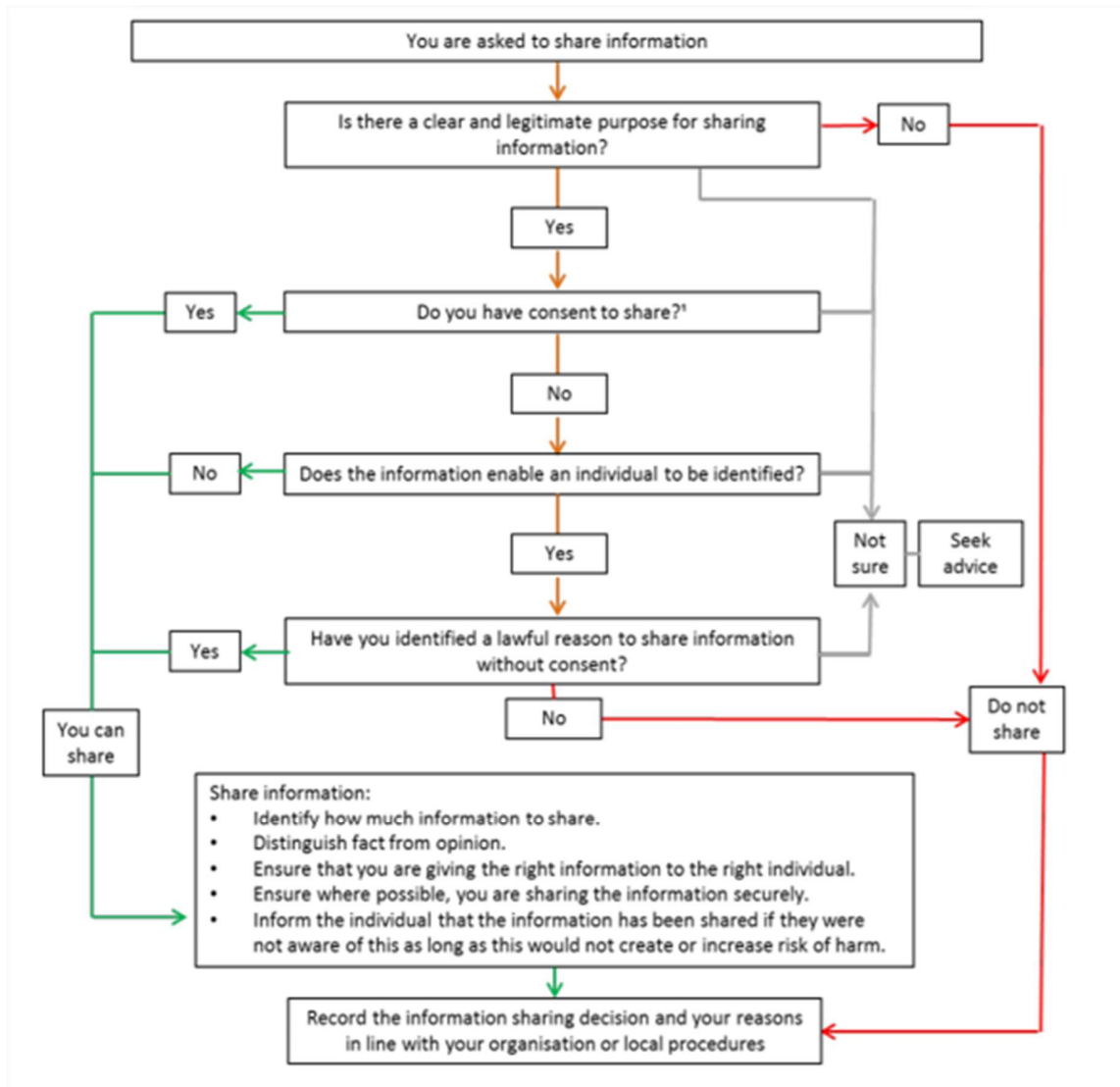
---

3 years.

## GDPR and Data Protection Policy

### Data Sharing Process Flow

The below diagram represents a typical process flow for UK GDPR data sharing, the controls relating to data sharing and the actions that should be taken before sharing data.





## GDPR and Data Protection Policy

---

### Subject Access Requests and Data Rights – Service users and Staff

#### Introduction

Under UK GDPR legislation, Data Controllers shall provide the information outlined in Articles 13 & 14 to Data Subjects and Data Subjects may access, correct, delete, restrict processing of, and transfer of their personal data, as well as object to automated decision-making based on their personal data.

#### SAR and Data Rights Procedure

Subject Access Requests should come to the email address [louise@maddcollege.co.uk](mailto:louise@maddcollege.co.uk) in the first instance and be followed up with an acknowledgement letter/email.

All requests and their progress must be logged by the Data Protection Officer in a secure place with no external access.

#### SAR Timescales

All Subject Access Requests will be completed within 30 days unless defined as complex – if the time will exceed 30 days, the requestor will be notified.

#### SAR Fees

Subject Access Requests coming directly from the data subject will be free, however, MADD can charge a fee if requests become unfounded or excessive. If requests are coming from a Service User on behalf of a data subject, MADD may charge a fee for data retrieval.

#### SAR Business Processes

The processes cover SAR and other data rights of individuals:

- Right of Access and Data Portability
- Right to Erasure
- Right to Object
- Right to Restriction
- Right to Rectification



## GDPR and Data Protection Policy

---

### Undertaking Privacy Impact Assessments

When MADD undertakes the use of new technologies or will be involved in the processing of data that contains a high risk to the rights and freedoms of data subjects, it will undertake a Privacy Impact Assessment.

The scale and nature of each PIA will be shaped on a case-by-case basis to capture the following information to inform the decision-making process:

- Risk Assessment
- Data types, collection, storage use and deletion methodologies
- Legal basis
- Information flows processes and procedures
- Consultation
- Evaluation of privacy procedures
- Final summary

For further information on PIA Please refer to:

<https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf>



## GDPR and Data Protection Policy

---

### Confidentiality

We do not disclose information given to us to third parties without consent unless required under our safeguarding policies and procedure or our obligations regarding the Data Protection Act 1998 and GDPR 2018/UK GDPR 2021.

All breaches will be taken seriously and are potentially a disciplinary matter.

There are, however, exemptions for breaches of confidentiality under special circumstances.

Any actual or suspected breaches of confidentiality shall be reported at once to the MADD Scheduling, Policy & Compliance Officer who will immediately:

- Risk assess the situation and determine what steps need to be taken.
- Immediately take such steps as are necessary to minimise the risk to Service users, Staff, and the charity.
- Take such steps as are necessary to ensure that similar breaches cannot happen again.

### Service Users

It is necessary to collect and keep a certain amount of information about our service users, however:

- We only collect and keep information that is necessary to enable us to perform our services.
- Access to the information held on service users is restricted to MADD staff.
- Information is not made available to third parties without the informed specific consent of the data subject (or by exceptions under the Data Protection Act 1998/UK GDPR).
- When collecting information, we should always inform data subjects why information is required and what it will be used for.
- Subcontractors working for MADD are also required to comply with our confidentiality policy.

## GDPR and Data Protection Policy

---

### Discussions and Meetings

- If discussing a person's situation in a meeting, Staff should only disclose information relevant to the matter at hand.
- Staff should be aware that others with no involvement may be able to overhear e.g., at reception, in an open-plan office or corridors. Staff will ensure discussions happen in an appropriate place.
- Staff will not discuss personal facts about one person with, or in the presence of, any other person unless within the scope and requirements of work.

### Outside of Work

- Staff should regard all information they have access to or are given because of their work for MADD as being always confidential unless advised otherwise.
- When working remotely, all personal and sensitive information should be kept in locked storage and should only be shared through secured systems, i.e., using password-protected documents, secure platforms, etc.

### Requests for Information

- People have a right to request access to information kept about them. The request must be in writing and dealt with by DPO.
- Third parties may request information about a person. This should only be given if we have received formal consent from the person.

### Security of Personal Data

MADD will ensure that personal data is held securely and for no longer than is necessary.

If you believe you have lost any personal data on any individuals in the course of your work, you must report it immediately.

Failure to do so may result in disciplinary action up to and including dismissal.



## GDPR and Data Protection Policy

---

### Disclosure Policy

MADD will not allow personal and sensitive personal data collected from service users to be disclosed to third parties except in circumstances that meet the requirements of our defined legal basis or other controls defined by GDPR.

Example situations are when:

- The person has consented to the disclosure.
- There is a serious risk of harm.
- Where MADD receives information that may prevent a crime or assist in the detection of a crime.
- Where MADD is legally obliged to disclose the data.

### Procedure on Disclosures

Any disclosure to be made must be checked for suitability beforehand and the individual performing the check may refer to the Information Commissioner for advice and guidance.

Any request for data based on a legal requirement, e.g., from the Police or other body, must be in writing and be checked by a member of the Senior Management against the advice of the Information Commissioner before any data is disclosed.





## GDPR and Data Protection Policy

---

### Staff Records

It is necessary to collect and keep a certain amount of information about current, former, and potential Staff.

Our confidentiality policy aims to safeguard privacy and ensure appropriate access to information:

- The processing of all information is governed by GDPR 2018/UK GDPR 2021.
- We only collect and keep the necessary information to perform roles and manage HR and payroll administration.
- Information is not made available to third parties without the informed consent of the staff member (or exceptions as in the Data Protection Policy or exceptions under the safeguarding policies and procedures).
- When collecting information from a staff member we should always inform them why information is required and what it will be used e.g., for supervision purposes.
- Personal facts about one staff member are not discussed with, or in the presence of, any other person.
- Staff will not disclose personal details (home address, telephone number etc.) to persons or other parties but should use their project address when an address must be given.

### Outside of Work

Staff must adhere to the Confidentiality and Data Protection policies and procedures at all times.

### Personal and Sensitive Information

MADD will process sensitive data, such as medical information and DBS checks, primarily where it is necessary to enable MADD to meet its legal obligations and in particular to ensure adherence to health and safety and vulnerable group protection legislation or for equal opportunities monitoring purposes.

MADD will not process sensitive personal data without consent.



## GDPR and Data Protection Policy

---

### Requests for Information

Staff have the same Subject Access Requests rights as service users.

### Disclosure Policy and Procedures

MADD will not allow personal and sensitive personal data collected from employees to be disclosed to third parties except in circumstances that meet the requirements of GDPR 2018/UK GDPR 2021.

This will be where because the employee has consented to the disclosure, there is a serious risk of harm, MADD receives information that may prevent a crime or assist in the detection of a crime, or MADD is legally obliged to disclose the data.

### Procedure on Disclosures

Any request for data based on a legal requirement, e.g., from the Police or other body, must be in writing and be checked by the relevant Manager, or a member of the Senior Management team and taking the advice of the Information Commissioner before any data is disclosed.

## Governance

This policy is owned and maintained by the MADD Senior Management.

## Monitoring and Reviewing

This policy should be reviewed periodically to ensure that it remains compliant with current legislation, meets best practices, and is not discriminatory.

Where we identify the need for modification of policy or if there are legal changes, they will be implemented; additional controls will be put in place and reflected in an updated version of this policy document.

The version number on new policies is always 1.0 and should be increased by one whole number each time the policy is edited other than to make simple changes, where they may increase in increments of 0.1.