# GDPR Data Protection Policy
# &
# Data Breach Procedure

| | |
|---|---|
| Date of Trust Board Approval | 10.05.2022 |
| Date of Consultation | n/a |
| Date of Issue | 01.05.2025 |
| Date of Next Review | 01.05.2027 |

## 1. Introduction

1.1 The Maritime Academy Trust (the **Trust**) is required to keep and process certain information about its Members, Trustees, Governors, staff members, pupils and their parents and carers in accordance with its legal obligations under the General Data Protection Regulation (**GDPR**).

1.2 The Trust may, from time to time, be required to share personal information held on the data subjects detailed above with other organisations.

1.3 This policy is in place to ensure that all staff members and Governors are aware of their responsibilities and outlines how the Trust complies with the core principles of the GDPR.

1.4 Organisational methods for keeping data secure are imperative, and the Trust believes that it is good practice to keep clear practical policies, backed up by written procedures.

## 2. Legal Framework

2.1 This policy has due regard to legislation, including, but not limited to the following:

(a) The General Data Protection Regulation;

(b) The Freedom of Information Act 2000;

(c) The Education (Pupil Information) (England) Regulations 2005 (as amended in 2016);

(d) The Freedom of Information and Data Protection (Appropriate Limit and Fees Regulations 2004); and

(e) The School Standards and Framework Act 1998.

## 3. Applicable Data

3.1 The GDPR applies to 'personal data' meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier. This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier. The GDPR applies to both automated personal data and to manual filing systems where personal data is accessible according to specific criteria.

3.2 The GDPR refers to sensitive personal data as "special categories of personal data". The following categories of data are included in this definition: racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation.

3.3 Personal data relating to criminal convictions and offences are not included, but similar extra safeguards apply to its processing.

## 4. Principles

4.1 The GDPR sets out the following data protection principles:

(a) data will be processed lawfully, fairly and in a transparent manner;

(b) data is collected for specified, explicit and legitimate purposes and not processed further in a manner incompatible with those purposes;

(c) data is adequate, relevant and limited to what is necessary for the purpose collected;

(d) data is accurate and kept up to date and that inaccurate data is erased without delay;

(e) data is kept in a form which permits identification of data subjects for no longer than is necessary for the purpose for which the data is processed;

(f) data is processed in a manner which ensures appropriate security of the data, including protection against unauthorised/unlawful processing and against accidental loss, destruction or damage.

## 5. Accountability & Governance

5.1 The Trust will implement appropriate technical and organisational measures to demonstrate that data is processed in accordance with the principles of the GDPR.

5.2 The Trust will maintain a register of data processing activities which will be reviewed on an annual basis. The register will include the following:

(a) categories of personal data held;

(b) purpose of data processing;

(c) legal basis for data collection;

(d) security measures in respect of the data;

(e) details of data transfers to third parties/countries;

(f) retention schedules.

5.3 The Trust will implement measures that meet the principles of data protection by design and data protection by default.

## 6. Data Protection Officer (DPO)

6.1 The Trust has appointed a Data Protection Officer (DPO) with professional experience and knowledge of data protection law in order to:

(a) inform and advise the Trust and its employees about their obligations to comply with the GDPR and other data protection laws; and

(b) monitor the Trust's compliance with the GDPR and other laws, including managing internal data protection activities, advising on data protection impact assessments, conducting internal audits, and ensuring that staff have received appropriate training.

6.2 The Data Protection Officer (DPO) will operate independently and will report directly to the Chief Executive Officer (CEO) and Board of Trustees.

## 7. Lawful Processing

7.1 The legal basis for processing data will be identified and documented prior to data being processed. In line with the requirements of Article 6 of the GDPR data processing will be lawful when the consent of the data subject has been obtained and when processing is necessary for one or more of the following reasons:

(a) compliance with a legal obligation;

(b) the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(c) for the performance of a contract with the data subject or to take steps to enter into a contract;

(d) protecting the vital interests of a data subject or another person;

(e) for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject.

7.2 The processing of sensitive data will have a legal basis in both Articles 6 and 9 of the GDPR and will be identified and documented prior to processing.

## 8. Consent

8.1 Consent can be withdrawn by a data subject at any time.

8.2 Where a child is aged under 16 the consent of parents will be sought prior to the processing of their data, except where the processing is related to preventative or counselling services offered directly to a child.

## 9. Rights of the Individual

9.1 The GDPR provides individuals with a number of rights in respect of how their personal data is processed:

**The right to be informed:**
Privacy notices provided in respect of data processing will be in clear plain language and accessible and will detail the identity and contact details of the controller and the DPO.

Privacy notices will set out the legal basis for processing the data and the legitimate interests of the controller. The rights of the data subject will also be detailed. The legal basis for holding the data and retention requirements will also be included.

**The right of access**
Individuals will have the right to submit a subject access request (SAR) to gain access to their personal data. In the first instance information will be supplied without charge, however, the Trust will reserve the right to impose a 'reasonable fee' for further requests for the same information.

All requests for data will be responded to within one month of receipt of the request, unless the request is complex in which case an extension of one month may be applied. The Trust reserves the right to refuse unfounded or excessive requests.

**The right to rectification**

Individuals will be entitled to have any inaccurate or incomplete data rectified. Where the personal data has been disclosed to a third party the Trust will inform them of the rectification if possible. Requests for rectification will be responded to within one month or two months where a request is deemed to be complex.

**The right to erasure**

Individuals will have the right to request the deletion of their data where there is no compelling reason for its continued processing. The right to request erasure will also apply where an individual withdraws their consent or when personal data has been unlawfully processed. The Trust has the right to refuse a request for erasure for the following reasons:

(a) to exercise the right of freedom of expression and information;

(b) to comply with a legal obligation for the performance of a public interest task or exercise of official authority;

(c) for public health purposes in the public interest;

(d) for archiving purposes in the public interest; or

(e) the exercise or defence of legal claims.

Special consideration will be given to existing situations where a child has given consent to processing and they later request erasure of the data.

Where personal data has been made public within an online environment the Trust will inform other organisations who process the data to erase links to and copies of the data.

**The right to restrict processing**

Individuals have the right stop or restrict the processing of their personal data. In the event that processing is restricted the Trust will store the personal data but not further process it.

The Trust will restrict the processing of personal data in the following circumstances where:

(a) an individual contests the accuracy of the personal data, processing will be restricted until the Trust has verified the accuracy of the data;

(b) an individual has objected to the processing and the Trust is considering whether their legitimate grounds override those of the individual;

(c) processing is unlawful and the individual opposes erasure and requests restriction instead;

(d) the Trust no longer needs the personal data but the individual requires the data to establish, exercise or defend a legal claim.

If the personal data has been disclosed to a third party the Trust will inform them about the restriction on the processing of the personal data.

**The right to data portability**
Individuals have the right to obtain and reuse their personal data across different services. Personal data may be moved, copied or transferred from one IT environment to another in a secure manner, in a structured, commonly used and machine readable format.

**Data Portability**
The right to data portability will apply in the following cases:

(a) to personal data that an individual has provided to a controller;

(b) where the processing is based on the individual's consent or for the performance of a contract;

(c) when processing is carried out by automated means.

The Trust is not required to adopt or maintain processing systems which are technically compatible with other organisations. The Trust will respond to requests for portability within one month. In the event that the request is complex the timescale may be extended by two months.

**The Right to Object**
The Trust will inform individuals of their right to object. This information will be included in privacy notices.

Individuals have the right to object to the following:

(a) processing based on legitimate interests or the performance of a task in the public interest;

(b) direct marketing;

(c) processing for purposes of scientific or historical research and statistics.

Where personal data is processed for the performance of a legal task or legitimate interests:

(a) an individual's grounds for objecting must relate to his or her particular situation;

(b) the Trust will stop processing the individual's personal data unless the processing is for the establishment, exercise or defence of legal claims, or, where the Trust can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual.

**Automated decision making and profiling**

Individuals have the right not to be subject to a decision when it is based on automated processing.

When automatically processing personal data the Trust will ensure that appropriate safeguards are in place, including:

(a) ensuring processing is fair and transparent;

(b) using appropriate mathematical or statistical procedures;

(c) implementing appropriate technical and organisational measures to enable inaccuracies to be corrected;

(d) securing personal data in a way that is proportionate to the risk to the interests and rights of the individual and prevents discriminatory effects.

Automated decisions must not concern a child or be based on the processing of sensitive data unless:

(a) the Trust has the explicit consent of the individual; or

(b) the processing is necessary for reasons of substantial public interest.

## 10. Data Protection Impact Assessments (DPIA)

10.1 A Data Protection Impact Assessment (DPIA) is a tool to help identify and minimise data protection risks. Conducting a DPIA meets, in part, an organisation's accountability obligations under GDPR, and is an integral part of the 'data protection by default and by design' approach.

10.2 The GDPR sets out an obligation to conduct a DPIA when:

- Using new technologies; and
- The processing is likely to result in a high risk to the rights and freedoms of individuals

Processing that is likely to result in a high risk includes (but is not limited to):

- Systematic and extensive processing activities, including profiling and where decisions have legal effects, or similarly significant effects, on individuals
- Large-scale processing of special categories of data or personal data relating to criminal convictions or offences
- Large-scale, systematic monitoring of public areas (such as CCTV)

10.3 A DPIA must:

- describe the nature, scope, context and purposes of the processing;
- assess necessity, proportionality and compliance measures;
- identify and assess risks to individuals; and
- identify any additional measures to mitigate those risks.

10.4 A DPIA does not have to eradicate the risks altogether, but should help to minimise risks and assess whether or not remaining risks are justified. In the event that a DPIA identifies a high risk that cannot be mitigated the ICO must be informed.

10.5 When conducting a DPIA advice should be sought from the Trust DPO who will be guided by the ICO requirements. A DPIA template is attached at Appendix 1 of this document.

## 11. Data Security

11.1 Confidential paper records will be kept in a locked filing cabinet, drawer or safe with restricted access. Paper records will not be left unattended anywhere with general access.

11.2 Digital data will be coded, encrypted or password-protected, both on a local hard drive and on a network drive that is regularly backed up off site.

11.3 Where data is saved on removable storage or a portable device the device will be kept in a locked filing cabinet, drawer or safe when not in use.

11.4 All electronic devices will be password protected to protect the information on the device in the event of loss or theft. Where possible the Trust will enable electronic devices to allow for remote blocking or deletion of data in the case of theft.

11.5 Memory sticks will not be used to hold personal data unless they are password protected and fully encrypted.

11.6 Staff members, Trustees and Governors must not download or store copies of personal data held by the Trust or any academy onto their personal laptops or computers.

11.7 All staff members will be provided with their own secure log in and password and every computer will regularly prompt users to change their passwords.

11.8 Emails containing sensitive or confidential information are password protected if there are unsecure servers between the sender and the recipient.

11.9 Circular emails to parents will be sent blind carbon copy (bcc) so that email addresses are not disclosed to other recipients.

11.10 Where personal data that could be considered private or confidential is taken off premises, either in electronic or paper format, staff will take extra care to follow procedures for security. The person taking the information accepts full responsibility for the security of the data.

11.11 Before sharing data all staff members will ensure:

(a) they are allowed to share it;

(b) that adequate security is in place to protect it; and

(c) the recipient of the data is detailed in the privacy notice.

11.12 Under no circumstances will visitors be allowed access to confidential or personal information. Visitors to the Trust or its academy premises must be supervised at all times and not allowed access to areas containing sensitive information.

11.13 The physical security of the Trust and its buildings, storage systems and access to them will be subject to regular review. If an increased risk of vandalism/burglary/theft is identified, extra measures to secure data storage will be put in place.

11.14 The Trust expects all staff members to comply with the statutory obligations of the GDPR. Any unauthorised disclosure by a member of staff may result in disciplinary action.

## 12. Data Breaches

12.1 A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data. This includes breaches that are the result of either accidental or deliberate causes.

12.2 Where a breach is likely to result in a 'risk' to the rights and freedoms of individuals the relevant supervisory authority will be informed within 72 hours of the Trust becoming aware of the breach.

12.3 In the event that a breach is likely to result in a 'high risk' to the rights and freedoms of an individual, the Trust will notify the subject(s) of the data breach without undue delay.

12.4 Within a breach notification, the following information will be outlined:

(a) the nature of the personal data breach, including the categories and approximate number of individuals and records concerned;

(b) the name and contact details of the DPO;

(c) an explanation of the likely consequences of the personal data breach;

(d) a description of the proposed measures to be taken to deal with the personal data breach;

(e) where appropriate, a description of the measures taken to mitigate any possible adverse effects.

12.5 The Trust will ensure that all staff members are aware of and understand what constitutes a data breach and the action they should take in the event that they become aware of a breach.

12.6 Following a breach a meeting will be convened by the DPO and relevant staff to review the breach, the process followed and agree measures to mitigate future breaches.

12.7 The data breach procedure is attached at Appendix 2 of this document.

## 13. CCTV and photography

13.1 The Trust acknowledges that recording images of identifiable individuals constitutes processing personal data. Processing of this type of data will be managed in line with the principles of the GDPR.

13.2 All Trust academies will notify pupils, staff and visitors of the purpose for collecting CCTV images via notice boards, letters and email.

13.3 Cameras are only placed where they do not intrude on anyone's privacy and are necessary to fulfil their purpose.

13.4 All CCTV footage will be kept for six months for security purposes; the School Business Manager will be responsible for keeping the records secure and allowing access.

13.5 If an academy within the Trust wishes to use images/video footage of pupils in a publication, such as its website, prospectus, or recordings of plays, written permission will be sought from the parent/carer of the pupil.

13.6 Images captured by individuals for recreational/personal purposes, and videos made by parents for family use, are exempt from the GDPR.

## 14. Biometric recognition systems

14.1 As a Trust we do not currently use pupils' biometric data as part of an automated biometric recognition system. If we do decide to implement this in the future we will comply with the requirements of the Protection of Freedoms Act 2012.

14.2 Parents/carers will be notified before any biometric recognition system is put in place or before their child first takes part in it. The Trust will get written consent from at least one parent or carer before we take any

biometric data from their child and first process it. Parents/carers and pupils have the right to choose not to use the Trust's biometric system(s). We will provide alternative means of accessing the relevant services for those pupils. Parents/carers and pupils can withdraw consent, at any time, and we will make sure that any relevant data already captured is deleted.

14.3 As required by law, if a pupil refuses to participate in, or continue to participate in, the processing of their biometric data, we will not process that data irrespective of any consent given by the pupil's parent(s)/carer(s).

14.4 Where staff members or other adults use the school's biometric system(s), we will also obtain their consent before they first take part in it, and provide alternative means of accessing the relevant service if they object. Staff and other adults can also withdraw consent at any time, and the Trust will delete any relevant data already captured.

## 15. Data Retention & Disposal

15.1 Data will not be kept for longer than is necessary and timescales for the retention of documents is set out in the Trust Retention Schedule.

15.2 Records relating to former pupils or employees of the Trust may be kept for an extended period for legal reasons, but also to enable the provision of references or academic transcripts.

15.3 Paper documents will be disposed of securely and electronic data deleted, once the data should no longer be retained.

## Appendix 1

### Data Protection Impact Assessment (DIPA) Template

This template sets out how to record a DPIA process and outcome. It follows the process set out in the ICO DPIA guidance.

The template should be completed at the start of any major project involving the use of personal data, or if you are making a significant change to an existing process. The outcomes should then feed back into project plans.

## Step 1: Identify the need for a DPIA

| Explain broadly what the project aims to achieve and what type of processing it involves. Summarise why you identified the need for a DPIA. |
| --- |
| |

## Step 2: Describe the processing

| **Describe the nature of the processing:** how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or other way of describing data flows. What types of processing identified as likely high risk are involved? |
| --- |
| |

| **Describe the scope of the processing:** what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover? |
| --- |
| |

| **Describe the context of the processing:** what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)? |
| --- |
| |

| **Describe the purposes of the processing:** what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for the organisation, and more broadly? |
| --- |
| |

## Step 3: Consultation process

| **Consider how to consult with relevant stakeholders:** describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within the organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts? |
| --- |
| |

## Step 4: Assess necessity and proportionality

| **Describe compliance and proportionality measures, in particular:** what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers? |
| --- |
| |

## Step 5: Identify and assess risks

| **Describe source of risk and nature of potential impact on individuals.** Include associated compliance and corporate risks as necessary. | **Likelihood of harm** | **Severity of harm** | **Overall risk** |
|---|---|---|---|
| | Remote, possible or probable | Minimal, significant or severe | Low, medium or high |

## Step 6: Identify measures to reduce risk

| **Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5** | | | | |
|---|---|---|---|---|
| **Risk** | **Options to reduce or eliminate risk** | **Effect on risk** | **Residual risk** | **Measure approved** |
| | | Eliminated<br>reduced<br>accepted | Low<br>medium<br>high | Yes/no |

## Step 7: Sign off and record outcomes

| Item | Name/date | Notes |
|---|---|---|
| Measures approved by: | | Integrate actions back into project plan, with date and responsibility for completion |
| Residual risks approved by: | | If accepting any residual high risk, consult the ICO before going ahead |
| DPO advice provided: | | DPO should advise on compliance, step 6 measures and whether processing can proceed |
| Summary of DPO advice: | | |
| DPO advice accepted or overruled by: | | If overruled, you must explain your reasons |
| Comments: | | |
| Consultation responses reviewed by: | | If your decision departs from individuals' views, you must explain your reasons |
| Comments: | | |
| This DPIA will kept under review by: | | The DPO should also review ongoing compliance with DPIA |

## Appendix 2
## Personal Data Breach Procedure

On being notified of, or finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the Trust Data Protection Officer (**DPO**). In practice breaches at school level will be reported to the Headteacher or School Business Manager in the first instance before being reported immediately to the DPO.

The DPO will investigate the report, and determine whether a breach has occurred.

The DPO will consider whether personal data has been accidentally or unlawfully:

- lost;
- stolen;
- destroyed;
- altered;
- disclosed or made available where it should not have been; or
- made available to unauthorised people.

The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary.

The DPO will determine if the breach must be reported to the Information Commissioners Office (ICO). This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:

- loss of control over their data;
- discrimination;
- identify theft or fraud;
- financial loss;
- unauthorised reversal of pseudonymisation (for example, key-coding);
- damage to reputation;
- loss of confidentiality; or
- any other significant economic or social disadvantage to the individual(s) concerned.

If it's likely that there will be a risk to people's rights and freedoms, the DPO will notify the ICO within 72 hours of the breach.

The DPO will document the decision, in case of challenge at a later date by the ICO or an individual affected by the breach. The DPO will maintain a register of all data breaches and reports to the Individual, subject to the breach and the ICO.

Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the DPO will set out:

- a description of the nature of the personal data breach including, where possible;
- the categories and approximate number of individuals concerned;
- the categories and approximate number of personal data records concerned;
- the name and contact details of the DPO;
- a description of the likely consequences of the personal data breach; and
- a description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned.

If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible.

The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:

- the name and contact details of the DPO;
- a description of the likely consequences of the personal data breach; and
- a description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned.

The DPO will notify any relevant third parties who can help mitigate the loss to individuals.

The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:

- facts and cause;
- effects; and
- action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals).

Following a data breach and as soon as is practicable a meeting will be convened by the DPO and relevant staff to review the reason for the breach, and agree measures to mitigate future breaches.

## Appendix 3

### Data Breach Process Flowchart