**ASHFORD INTERNATIONAL MODEL RAILWAY**

**EDUCATION CENTRE**

A PROJECT BY ASHFORD MODEL RAILWAY MUSEUM

REGISTERED CHARITY 1168774

POLICY STATEMENT AND PROCEDURE FOR GDPR AND INFORMATION SECURITY

Document Reference AIMREC/P02

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Issue No | Date | by | Approved | Notes |
| 1 | 09-02-2022 | Nigel Hoad | Fred Garner | First Issue |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Unit 2 Mill Farm Business Units, Fridd Lane, Bethersden, Kent, TN26 3DB

Tel 01233 333877

|  |  |
| --- | --- |
| **Contents**  **AIMREC GDPR and Information Security Policy Statement Page 3**  **AIMREC GDPR and Information Security Procedure Page 4**    **APPENDIX 1 – Review Form Page 11**  **APPENDIX 2 – Data Register Page 12**  **APPENDIX 3 – Audit Form Page 13**  **APPENDIX 4 – Consent Form Page 16**  **APPENDIX 5 – Privacy Notice Page 17**  **APPENDIX 6 – Induction Training Page 19** |  |

**AIMREC GDPR and Information Security Policy Statement**

AIMREC’s Directors and Trustees take Information Security and compliance with GDPR requirements seriously. We will treat all information collected by AIMREC in the course of its activities as a charity, model railway visitor attraction and educational venue in accordance with the General Data Protection Regulations and Data Protection Legislation.

We will appoint and train all persons who are required to process information on behalf of AIMREC in the requirements of this Policy and Procedure. Information collected by AIMREC is to be treated with confidentiality; unauthorised access and disclosure is to be prevented; information integrity is to be maintained; accuracy safeguarded and access only for authorised users.

AIMREC take privacy and information security concerns seriously. If you have any concerns about the way your information is being handled, please contact the Data Protection Officer without delay. We will carefully investigate and review all complaints and take appropriate action in accordance with Data Protection Legislation. We will keep you informed of the progress of our investigation and the outcome.

If you are not satisfied with the outcome, you may wish to contact the Information Commissioner’s Office at https://ico.org.uk/concerns/

Our Data Protection Officer is Mr Rupert Brown who is responsible for the implementation and supervision of this Policy and accompanying Procedures. His contact e mail is rupertb@cix.co.uk

Signed by

…………………………. Data Protection Officer

**AIMREC GDPR and Information Security Procedure**

**1.0 Definitions**

|  |  |
| --- | --- |
| “Data Protection Legislation” or “Legislation” | means the Data Protection Act 1998, the Privacy and Electronic Communications Regulations (EC Directive) Regulations 2003 (SI 2426/2003 as amended), the General Data Protection Regulation (GDPR), any laws in the UK enacting the GDPR or preserving its effect in whole or part following the departure of the UK from the European Union and all applicable laws and regulations, including any replacement UK or EU data protection legislation relating to the Processing of Personal Data, together with, where applicable, the guidance and codes of practice issued by the Information Commissioner’s Office. |

**2.0 Legislation**

2.1 Data Protection Legislation is concerned with the protection of human rights in relation to personal data. The aim of the Legislation is to ensure that personal data is used fairly and lawfully and that where necessary the privacy of individuals is respected. During the course of the activities of AIMREC, we will collect, store and process personal data about our trustees, volunteers, people who attend our events and activities, suppliers and other third parties and we recognise that the correct and lawful treatment of this data will help maintain confidence in AIMREC. This procedure sets out the basis on which we will process any personal data we collect from data subjects, or that is provided to us by data subjects or other sources.

2.2 The Data Protection Compliance Manager is responsible for ensuring compliance with the Legislation and with this policy. The post is held by Rupert Brown.

2.3 Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the Data Protection Compliance Manager.

**3.0 Compliance with the Legislation**

3.1 Volunteers who process data on our behalf have a responsibility for processing personal data in accordance with the Legislation. This includes the data protection principles in the Legislation. These state that personal data must:

* be obtained and used fairly, lawfully, and transparently
* be obtained for specified, explicit and legitimate purposes and used only for those purposes
* be adequate, relevant, and limited to the minimum necessary for those purposes
* be accurate and kept up to date (every reasonable endeavour should be used to personal data that is not accurate is corrected or erased without delay)
* be processed in a manner that ensures its security (*see Information Security Policy at Appendix 1).*
* not be kept for any longer than required for those purposes *see Retention Policy at Appendix 2).*

3.2 We will only share personal data with other organisations or people when we have a legal basis to do so and if we have informed the data subject about the possibility of the data being shared (in a privacy notice) unless there is a legal exemption from doing so. We will keep records of any information shared with a third party including a record of any exemption which has been applied.

3.3 Volunteers should follow the Data Breach Procedure *(at Appendix 3)* if they think they have accidentally breached any provision of this Data Protection Policy.

**4.0 Processing personal data**

4.1 All personal data will be processed in accordance with the Legislation and this policy. Any breach of this policy may result in disciplinary action. Processing includes obtaining, holding, maintaining, storing, erasing, blocking, and destroying data.

4.2 Personal data is data relating to a living individual and includes employee, volunteer, and visitor data. It does not include data relating to a company or organisation, although any data relating to individuals within companies or organisations may be covered. Personal data can be factual (for example a name, address, or date of birth) or it can be an opinion about that person, their actions and behaviour.

4.3 Examples of personal data are volunteer details, including names and addresses and other information relating to individuals, including supplier details, any third-party data and any recorded information including any recorded telephone conversations, emails, or CCTV images.

4.4 Volunteers and others (including trustees) who process data on behalf of AIMREC (referred to in this policy as ‘Volunteers’) should assume that whatever they do with personal data will be considered to constitute processing.

4.5 Volunteers will only process data:

* If they have consent to do so; or
* If it is necessary to fulfil a contractual obligation or as part of the employer/employee relationship; for example, processing the payroll; or
* the processing is **necessary for legitimate interests** pursued by AIMREC unless these are overridden by the interests, rights, and freedoms of the data subject.

If none of these conditions are satisfied, individuals should contact the Data Protection Compliance Manager before processing personal data.

**5.0 IT Systems and Data Processing**

5.1 Our IT systems will only be used for authorised purposes, and they will be monitored regularly.

5.2 We will take appropriate technical and organisational steps to guard against unauthorised or unlawful processing. In particular:

* All data will be stored in a secure location and precautions will be taken to avoid data being accidentally disclosed.
* Manual records relating to Centre volunteers, trustees, or visitors will be kept secure in locked cabinets. Access to such records will be restricted.
* Access to systems on which information is stored must be password protected with strong passwords and these should be changed at once if there is a risk they have been compromised. Passwords must not be disclosed to others.
* We will ensure that trustees and volunteers who handle personal data are adequately trained and monitored to ensure data is being kept secure.
* We will ensure that only those who need access will have access to data.
* We will take particular care of sensitive data and security measures will reflect the importance of keeping sensitive data secure (definition of sensitive data is set out above in the Data Protection Policy), e.g. password protection for documents and encryption.
* Where personal data needs to be deleted or destroyed adequate measures will be taken to ensure data is properly and securely disposed of. This will include destruction of files and back up files and physical destruction of manual files. Particular care should be taken over the destruction of manual sensitive data (written records) including shredding or disposing via specialist contractors (who will be treated as data processors -see below).
* We will ensure that any data processor engaged to process data on our behalf (e.g. for payroll) will act under a written contract and will give appropriate undertakings as to the security of data.
* Appropriate software security measures will be implemented and kept up to date.
* We will ensure that if information has to be transported or transferred, this is done safely using encrypted devices or services.
* Where personal devices are used to store or process personal data, they must be subject to appropriate security.

All breaches of this policy must be reported to the Data Protection Compliance Manager

**6.0 Monitoring the use of personal data**

6.1 We are committed to ensuring that this data protection procedure is put into practice and that appropriate working practices are being followed. To this end the following steps will be taken:

* any Volunteers who deal with personal data are expected to be aware of data protection issues and to work towards continuous improvement of the proper processing of personal data.
* Volunteers who handle personal data on a regular basis or who process sensitive or other confidential personal data will be more closely monitored.
* All Volunteers must consider whether the personal data they hold is being processed in accordance with this policy. Particular regard should be had to ensure inaccurate, excessive, or out of date data is disposed of in accordance with this policy.
* Volunteers must follow the Breaches Procedure (*at Appendix 3)* should they become aware of any breach of this policy.
* Volunteers will keep clear records of our processing activities and of the decisions we make concerning personal data (including reasons for the decisions) to show how we comply with the Legislation.
* Spot checks may be carried out.
* An annual report on the level of compliance with or variance from good data protection practices will be produced by Fiona Strasser
* Data breaches will be recorded and investigated to see what improvements can be made to prevent recurrences.
* We will only appoint data processors on the basis of a written contract that will require the processor to comply with all relevant legal requirements. We will continue to monitor the data processing, and compliance with the contract, throughout the duration of the contract.

**7.0 Sensitive data**

7.1 We will strive to ensure that sensitive data is accurately identified on collection so that proper safeguards can be put in place. Sensitive data means data consisting of information relating to an individual’s

* Racial or ethnic origin
* Political opinions
* Religious beliefs
* Trade union membership
* Physical or mental health, and genetic information
* Sexual life
* Criminal offences

Sensitive data may be processed in the course of our legitimate activities but may not be passed to any third party without the express consent of the data subject.

**8.0 The rights of individuals**

8.1 The Legislation gives individuals certain rights to know what data is held about them and what it is used for. If personal data is collected directly from an individual, we will inform them in writing of their rights by providing them with a ‘Privacy Notice’ at the time the personal data is collected or as soon as possible afterwards.

8.2 In principle everyone has the right to see copies of all personal data held about them. There is also a right to have any inaccuracies in data corrected or erased. Data subjects may also have a right of portability in respect of their personal data, and a right to be forgotten. Data subjects also have the right to prevent the processing of their data for direct marketing purposes.

8.3 Any request for access to data under the Legislation should be made to the Data Protection Officer in writing. In accordance with the Legislation we will ensure that written requests for access to personal data are complied with within **30 days** of receipt of a valid request (where permitted under the Legislation, we may take a further 30 days to respond but we will inform the individual of why this is necessary).

8.4 When a written data subject access request is received the data subject will be given a description of a) the personal data, b) the purposes for which it is being processed, c) those people and organisations to whom the data may be disclosed, d) be provided with a copy of the information in an intelligible form.

# 9.0 Storage of Data and Records

# 9.1 All data and records will be stored in accordance with the security requirements of the Data Protection Legislation and in the most convenient and appropriate location having regard to the period of retention required and the frequency with which access will be made to the record.

9.2 Data and records which are active should be stored in the most appropriate place for their purpose commensurate with security requirements.

9.3 Data and records which are no longer active, due to their age or subject, should be stored in the most appropriate place for their purpose or destroyed.

9.4 The degree of security required for file storage will reflect the sensitivity and confidential nature of any material recorded.

9.5 Any data file or record which contains personal data of any form can be considered as confidential in nature.

9.6 Data and records should not be kept for longer than is necessary. This principle finds statutory form in the Data Protection Legislation, which requires that personal data processed for any purpose "shall not be kept for longer than is necessary for that purpose". All trustees, and volunteers are required to have regard to the Guidelines for Retention of Personal Data attached hereto.

9.7 Any data that is to be disposed must be safely disposed of for example by shredding. Any group which does not have access to a shredder should pass material to the Data Protection Compliance Manager who will undertake secure shredding.

9.8 Special care must be given to disposing of data stored in electronic media.

## Guidelines for Retention of Personal Data

If you have any queries regarding retaining or disposing of data, please contact the Data Protection Compliance Manager

**Types of Data Suggested Retention Period**

|  |  |
| --- | --- |
| Personnel files  including training records and notes of disciplinary and grievance hearings. | * 6 years from the end of involvement |
| Application forms / interview notes | * Maximum of one year from the date of the interviews for those not subsequently accepted. If accepted, retain in personnel file. |
| Trustee information | * Check for accuracy once a year * Secure destruction of personal data other than name – three years after cease to be a Trustee |
| Income Tax, including correspondence with tax office | * At least 6 years after the end of the financial year to which the records relate |
| Accident books, and records and reports of accidents | * For Adults - 3 years after the date of the last entry * For children - three years after the child attains 18 years (RIDDOR 1985) |
| Safeguarding disclosure information | * Permanently |

**10 Breaches of Data**

10.1 AIMREC (“we”) hold and process personal data which needs to be protected, and compromise of information, confidentiality, integrity, or availability may result in harm to individuals, reputational damage, detrimental effect on service provision, legislative non-compliance and financial penalties.

10.2 A data breach is an event or action which may compromise the confidentiality, integrity or availability of systems or data, either accidentally or deliberately, and has caused or has the potential to cause damage to data subjects.

An incident includes but is not restricted to:

• Loss or theft of personal data or the equipment on which the data is stored e.g. laptop, memory stick, smartphone, or paper record

• theft or failure of equipment on which personal data is stored

• Unauthorised use of or access to personal data

• Attempts to gain unauthorised access to personal data

• Unauthorised disclosure of personal data

• Website defacement

• Hacking attack

10.3 Any person using personal data on behalf of AIMREC is responsible for reporting data breach incidents immediately to the Data Protection Officer or in his or their absence a Director. The report should contain the following details:

• Date and time of discovery of breach

• Details of person who discovered the breach

• The nature of the personal data involved

• How many individuals’ data is affected

10.4: The Data Protection Officer will first ascertain if the breach is still occurring. If so, appropriate steps will be taken immediately to minimise the effects of the breach. An assessment will be carried out to establish the severity of the breach and the nature of further investigation required. Consideration will be given as to whether the police should be informed. Advice from appropriate experts will be sought if necessary. A suitable course of action will be taken to ensure a resolution to the breach.

10.5 An investigation will be carried out without delay and where possible within 24 hours of the breach being discovered. [insert named individual] will assess the risks associated with the breach, the potential consequences for the data subjects, how serious and substantial those are and how likely they are to occur.

The investigation will consider the following:

• The type of data involved and its sensitivity

• The protections in place (e.g. encryption)

• What has happened to the data

• Whether the data could be put to illegal or inappropriate use

• Who the data subjects are, how many are involved, and the potential effects on them

• Any wider consequences

10.6 The Data Protection Officer will decide with appropriate advice who needs to be notified of the breach. Every incident will be assessed on a case-by-case basis. The Information Commissioner will be notified, if at all possible, within 24 hours of the data breach, if a large number of people are affected or the consequences for the data subjects are very serious.

10.7 Guidance on when and how to notify the ICO is available on their website https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/

10.8 Where appropriate, we will notify the data subjects whose personal data has been affected by the incident; such a notification may include a description of how and when the breach occurred, and the nature of the data involved, and specific and clear advice on what they can do to protect themselves and what has already been done to mitigate the risks.

10.9 The Data Protection Officer will keep a record of all actions taken in respect of the breach.

10.10 Once the incident is contained, the Data Protection Officer will carry out a review of the causes of the breach, the effectiveness of the response, and whether any changes to systems, policies or procedures should be undertaken. Consideration will be given to whether any corrective action is necessary to minimise the risk of similar incidents occurring. This action should be recorded.

**11.0 Changes to this Procedure**

11.1 We reserve the right to change this procedure at any time, including as needed to comply with changes in law. Where appropriate we will notify data subjects of those changes by mail or email.

**APPENDIX 1 - Data Protection Review Form**

All personal data that AIMREC holds needs to be reviewed annually. Please use this form to review the data you hold.

The ‘data subject’ is the person whose data you are dealing with. ‘Processing’ means using the data after it has been collected (e.g. contacting someone to advertise an event). If this is a person under 16 years of age, you should answer the questions with regard to the person’s parent or guardian. Anyone completing this questionnaire should first read the Data Protection Policy.

Please tick appropriate box

|  |  |  |  |
| --- | --- | --- | --- |
|  | Yes | No | N/A |
| Has the data subject been informed of processing? |  |  |  |
| Has the data subject been informed of third parties to whom their data may be provided? |  |  |  |
| Has the data subject given their consent to the processing? |  |  |  |
| If the data subject has not given consent (or consent is not a sufficient ground for processing) is processing justified by data controller’s legitimate interest? |  |  |  |
| If the data is sensitive data has the data subject given explicit consent? |  |  |  |
| Has the data subject been informed of the purpose(s) for processing? |  |  |  |
| Is there a clear ground for processing each item of data? |  |  |  |
| Is the information gathered no more than is necessary for the purpose(s)? |  |  |  |
| Are steps taken to ensure data is accurate? |  |  |  |
| Is there a system of rolling reviews to keep data up to date? |  |  |  |
| Is there a data retention policy for this data? |  |  |  |
| Is there a justification for retaining the data for the period in question? |  |  |  |
| Has the data subject been informed of their right of access? |  |  |  |
| Is the level of security applied to the data appropriate to the risks represented by the nature of the data to be protected (give consideration to possibility of theft, malicious damage or corruption including computer viruses, unlawful access, accidental disclosure, loss and destruction)? |  |  |  |
| Are those who deal with personal data aware of purposes for which it has been collected? |  |  |  |
| Are those who process data aware of parties to whom they can legitimately disclose it? |  |  |  |
| Where consultants and contractors have access to the data is there a written statement in place governing their obligations regarding security and use of data? |  |  |  |
| Are appropriate measures in place for the secure disposal and/or destruction of personal data no longer required? |  |  |  |
| Where applicable has consent of the data subject been obtained to transfer personal data to countries outside the EEA? |  |  |  |

Review carried out on ……………………………………………….

by………………………………………………………………………

**APPENDIX 2 - AIMREC Data Register**

All held data is audited on a yearly basis by the Data Controller with the Data Processors of each area detailed below

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **What Data is processed?** | **The purpose?** | **Who processes the data?**  **(Data Processor)** | **Stored where?** | **How long is data held?** | **Consent needed?** | **Lawful basis for No consent** |
| Trustees | | | | | | |
| Volunteers Names, addresses, phone numbers | To carry out duties of care | Trustees | Password protected electronic device  Locked filing cabinet | All the time the volunteer attends AIMREC events | NO | Legitimate interests |
| Events Co-Ordinator | | | | | | |
| Visitors | To notify about future events | Trustees | Password protected electronic device  Locked filing cabinet | 24 months | NO | Legal Obligation |
| Safeguarding | | | | | | |
| Volunteer application & reference request forms | To meet safer recruitment guidelines as stated in Safeguarding Policy | Safeguarding Lead | Password protected electronic device  Locked filing cabinet | All the time the volunteer attends AIMREC events | NO | Legitimate interests |
| DBS Forms | Law requires all Trustees and those working with others to hold a valid DBS | Safeguarding Lead | Password protected electronic device  Locked filing cabinet |  | NO | Legal Obligation |
| Disclosure Report Forms | To ensure AIMREC meets its duty in safeguarding | Safeguarding Lead | Password protected electronic device  Locked filing cabinet | Indefinitely | NO | Legal Obligation |
| Finance | | | | | | |
| Volunteers’ details, name, expenses etc | Details required for HMRC | Treasurer | Password protected electronic device  Locked filing cabinet | All the time the volunteer attends AIMREC events | NO | Legal Obligation |
| Volunteers bank details | Required for reimbursement for monies spent for the purpose of AIMREC | Treasurer | Password protected electronic device  Locked filing cabinet | All the time the volunteer attends AIMREC events | NO | Legitimate Interests |

**APPENDIX 3 - Data Protection Audit Form**

Please complete this form about the personal data you currently hold or collect on behalf of AIMREC

|  |  |
| --- | --- |
| Name of the person who collects/holds the data |  |
| Position in AIMREC |  |
| Contact details |  |
| Date of Audit |  |

**Data classes** – *what sort of data do you hold?* (Tick all that apply)

|  |  |
| --- | --- |
| Personal details |  |
| Family, lifestyle, social circumstances |  |
| Employment details |  |
| Financial details |  |
| Racial or ethnic origin |  |
| Political opinions |  |
| Religious or similar beliefs |  |
| Trade union membership |  |
| Physical or mental health or condition |  |
| Sexual life |  |
| Criminal proceedings, outcomes etc |  |
| Education and training |  |
| Other (please specify) |  |

**Data subjects** – *who is the data about?* (Tick all types that apply)

|  |  |
| --- | --- |
| Volunteers |  |
| Suppliers |  |
| Correspondents, enquirers and regular contacts |  |
| Relatives, guardians and associates of data subject |  |
| Children aged under 16 |  |
| Complainants |  |
| Others (please specify) |  |

**Data sources** – *How did you obtain that information?* (Tick)

|  |  |
| --- | --- |
| Data subject (who the data is about) |  |
| Third party (please specify) |  |

|  |  |
| --- | --- |
| **Locations of data** – *Please list the places you keep the data* |  |

**Format of data -** *What format do you keep the data in?* (Tick all that apply)

|  |  |
| --- | --- |
| Computer |  |
| Paper |  |
| Photograph |  |
| CCTV |  |
| Audio |  |
| Other (please specify)………………………………………. |  |

**Purpose(s) for which data processed** (e.g. to keep in contact with visitors)

**Data recipients** – *Are you sharing this with anyone outside of AIMREC?*

|  |  |
| --- | --- |
| Data subject (who the data is about) |  |
| Relatives, guardian or associate of data subject |  |
| Current, past or prospective employer of data subject |  |
| Employees and agents of data controller (who collects the data) |  |
| Education and training establishments |  |
| Suppliers |  |
| Persons making an enquiry or complaint |  |
| Voluntary and charitable organisations |  |
| Religious organisations |  |
| Regulatory authorities |  |
| Other (please specify) |  |

Transfers overseas – *Do you transfer any of this data overseas?*

|  |  |
| --- | --- |
| None outside EEA |  |
| Worldwide |  |
| Specific countries outside EEA (please name): |  |
|  |  |
|  |  |

Is any data processed by third parties on behalf of Data Controller? Yes/No (please indicate)

If yes, give details of data processor……………………………………………………………………………………

# APPENDIX 4 - Consent Form

|  |  |
| --- | --- |
| **Name** |  |
| **Address** |  |
| **Phone number** |  |
| **Email** |  |

By filling in this form, you are consenting to AIMREC holding your/your child’s information.

You can ask for your details to be removed at any time by contacting us at fred.garner@aimrec.co.uk.

We are collecting this information to enable us to contact you of events that we will organise in the future. We would like to send you information about our events and activities by post, telephone, email and text. If you agree to being contacted in this way, please tick the relevant boxes

Post

Email

Phone

Text

If you wish to stop receiving communications from us at any time, please contact us at fred.garner@aimrec.co.uk.

We do not share your information with third parties unless the law requires us to do so.

You have the right to request access to your personal data that we hold. For more information about this and other individual rights regarding personal data please see our website and our Privacy Notice.

**APPENDIX 5 - Privacy Notice**

**How AIMREC uses your information**

Your privacy is important to us. We are committed to safeguarding the privacy of your information.

It is important that you read this privacy notice together with any other privacy notice we may provide on specific occasions when we are collecting or processing personal data about you so that you are fully aware of how and why we are using your data.

**Why are we collecting your data?**

We collect personal data to provide appropriate pastoral care, to monitor and assess the quality of our services, to fulfil our purposes as a church and to comply with the law. In legal terms this is called ‘legitimate interests’. When it is required, we may also ask you for your consent to process your data. We do not share your information with others except as described in this notice.

**The categories of information that we may collect, hold and share include:**

* Personal information (such as name, telephone number, address, and email address)
* Characteristics (such as gender, ethnicity, language, nationality, country of birth)

**Storing your data**

We will only retain your personal data for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting or reporting requirements.

We hold your data for varying lengths of time depending on the type of information in question but in doing so we always comply with Data Protection legislation. Details of retention periods are available in our retention policy which you can request by contacting the Data Protection Compliance Manager

We will contact you annually to check that the information we are holding is accurate and that you agree to us holding it.

**Security of your data**

We have put in place appropriate security measures to prevent your personal data from being accidentally lost, used, or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal data to those employees or trustees who need to know. They will only process your personal data on our instructions.

We have put in place procedures to deal with any suspected personal data breach and will notify you and the Information Commissioner’s Office where we are legally required to do so.

**Who do we share your information with?**

We will not share your information with third parties without your consent unless the law requires us to do so.

**Requesting access to your personal data**

Under Data Protection legislation, you have the right to request access to information about you that we hold. To make a request for your personal information contact the Data Protection Compliance Manager.

You also have the right to:

* object to processing of personal data that is likely to cause, or is causing, damage or distress
* prevent processing for the purpose of direct marketing
* object to decisions being taken by automated means
* in certain circumstances, have inaccurate personal data rectified, blocked, erased, or destroyed; and
* claim compensation for damages caused by a breach of the Data Protection regulations.

For further information on how your information is used, how we maintain the security of your information and your rights to access information we hold on you please contact the Data Protection Compliance Manager.

If you have a concern about the way we are collecting or using your personal data, you should raise your concern with us in the first instance or directly to the Information Commissioner’s Office at <https://ico.org.uk/concerns/>

**Data Protection Compliance Manager & Contact**

Mr Rupert Brown is the Data Protection Compliance Manager and responsible for your personal data.

They can be contacted at: rupertb@cix.co.uk.

**APPENDIX 6 -** Data Protection Induction Checklist

An induction briefing for Directors, Trustees, Employees, and volunteers who collect or process data for AIMREC.

1. Introduction to data protection legislation – explain what GDPR is and why it has been introduced.

2. Data collection

* + What data do they collect? - review data audit with them
  + Explain the different legal conditions for processing data. What legal basis do they have for processing this data?
  + Do they need to get consent for this type of data when they collect any new data? Review form they currently use to collect data.
  + Run through the key points in AIMREC’s **data protection policy**.

3. Privacy notice

* Explain what information needs to be provided to the individuals and when.

4. Security

* + How do they store the data? Computers should be password protected
  + They should not pass data onto any third parties unless instructed by a director of AIMREC to do so.

5. Accuracy review

* + You need to regularly review data for accuracy. Plan together to do this. We recommend this is done annually.

6. Retention of Records

* + Data should not be kept longer than necessary. Do they know how long to keep the data for? Do they know what to do when they are deleting or getting rid of the data? Refer to the **Retention of Records Policy** for this.

7. Complaint’s procedure and breaches

* + Staff and volunteers should know what to do when there is a data breach or when there is a complaint concerning data protection. Refer to the **Complaints & Grievance Procedures**.

8. Discuss the process in AIMREC should you have a subject access request

9. Record the training in some way so you have proof that it took place.