JADC
Data Protection Policy

Last updated and approved:
25th January 2020

Next due for review and approval:
January 2021

Contents

1 PURPOSE

This policy establishes an effective, accountable and transparent framework for ensuring the Jersey Amateur Dramatic Club compliance with the requirements of the Data Protection (Jersey) Law 2018.

2 SCOPE

This policy applies to all Committee members and general members who have a responsibility for the processing of personal data on behalf of the Jersey Amateur Dramatic Club (referred to as "JADC", "we" or "us") and for the purpose of this policy, the JADC are the data controllers and we are pleased to provide you with the following Data Protection Policy.

.

3 POLICY STATEMENT

We are committed to conducting our club in accordance with all applicable data protection laws and regulations and in line with the highest standards of ethical conduct.

This policy sets forth the expected behaviours of our Committee and members in relation to the collection, use, retention, transfer, disclosure and destruction of any personal data belonging to a member, supporter or supplier (i.e. the data subject).

Personal data is any information (including opinions and intentions) which relates to an identified or identifiable natural person. Personal data is subject to certain legal safeguards and other regulations, which impose restrictions on how organisations may process personal data. An organisation that handles personal data and makes decisions about its use is known as a Data Controller. We, as a Data Controller, are responsible for ensuring compliance with the data protection requirements outlined in this policy. Non-compliance may expose us to complaints, regulatory action, fines and/or reputational damage.

Our committee are fully committed to ensuring continued and effective implementation of this policy and expects all members to share in this commitment. Any breach of this policy will be taken seriously and may result in disciplinary action.

Compliance Monitoring

To confirm that an adequate level of compliance that is being achieved by all members in relation to this policy, the Data Protection Advisor will carry out an annual data protection compliance audit for all processing activities. Each audit will, as a minimum, assess:

- Compliance with policy in relation to the protection of personal data, including:
- The assignment of responsibilities.
  - ✓ Raising awareness.
- The effectiveness of data protection related operational practices, including:
  - ✓ Data subject rights.
  - ✓ Personal data transfers.

- ✓ Personal data incident management.
- ✓ Personal data complaints handling.
- ✓ The level of understanding of data protection policies and privacy notices.
- ✓ The accuracy of personal data being stored.
- ✓ The conformity of data processor activities.

4 Data Protection Principles

We have adopted the following principles to govern our collection, use, retention, transfer, disclosure and destruction of personal data:

Principle 1: Lawfulness, Fairness and Transparency. Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject. This means, we must tell the data subject what processing will occur (transparency), the processing must match the description given to the data subject (fairness), and it must be for one of the purposes specified in the applicable data protection regulation (lawfulness).

Principle 2: Purpose Limitation. Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. This means we must specify exactly what the personal data collected will be used for and limit the processing of that personal data to only what is necessary to meet the specified purpose.

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

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

Principle 5: Storage Limitation. Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed. This means we must, wherever possible, store personal data in a way that limits or prevents identification of the data subject.

Principle 6: Integrity & Confidentiality. Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing, and against accidental loss, destruction or damage. We must use appropriate technical and organisational measures to ensure the integrity and confidentiality of personal data is maintained at all times.

Principle 7: Accountability. The JADC shall be responsible for and be able to demonstrate compliance. This means we must demonstrate that the six data protection principles (outlined above) are met for all personal data for which we are responsible.

5 Data collection

Data subject consent

We will obtain personal data only by lawful and fair means and, where appropriate with the knowledge and consent of the individual concerned. Where a need exists to request and receive the consent of a member prior to the collection, use or disclosure of their personal data, we are committed to seeking such consent. The Data protection Advisor, in cooperation with committee, shall establish a system for obtaining and documenting members consent for the collection, processing, and/or transfer of personal data.

Data subject Notification

We will, when required by applicable law, contract, or where it considers that it is reasonably appropriate to do so, provide members with information as to the purpose of the processing of their personal data. When the member is asked to give consent to the processing of personal data and when any personal data is collected from the members, all appropriate disclosures will be made, in a manner that draws the processing to theirattention, unless one of the following apply:

- The data subject already has the information;
- A legal exemption applies to the requirements for disclosure and/or consent. The disclosures may be given orally, electronically or in writing. If given orally, the person making the disclosures should use a suitable script. The associated receipt or form should be retained, along with a record of the facts, date, content, and method of disclosure.

External Privacy Notices

We will display a copy of the 'Privacy Notice' on our website, fulfilling the requirements of applicable law.

6 Data Use

Data processing

We use the personal data of our members for the following broad purposes:

- The general running of our club.
- To provide services to our members.
- The ongoing administration and management of member services.

The use of members information should always be considered from their perspective and whether the use will be within their expectations or if they are likely to object.

We will process personal data in accordance with all applicable laws and applicable contractual obligations. More specifically, We will not process personal data unless at least one of the following requirements are met:

- The data subject has given consent to the processing of their personal data for one or more specific purposes.
- Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.
- Processing is necessary for compliance with a legal obligation to which the JADC is subject.

- Processing is necessary for the purposes of the legitimate interests pursued by the JADC or by a third party (except where such interests are overridden by the interests or fundamental rights and freedoms of the member, in particular where the member is a child).

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

- In any circumstance where consent has not been gained for the specific processing in question, we will address the following additional conditions to determine the fairness and transparency of any processing beyond the original purpose for which the personal data was collected: Any link between the purpose for which the personal data was collected and the reasons for intended further processing.
- The context in which the personal data has been collected, in particular regarding the relationship between data subject and the JADC.
- The nature of the personal data, in particular whether special categories of data are being processed, or whether personal data related to criminal convictions and offences are being processed.
- The possible consequences of the intended further processing for the member.
- The existence of appropriate safeguards pertaining to further processing, which may include encryption, anonymisation or pseudonymisation.

High level Data Processing Activity Register can be found at Appendix B.

Special Categories of Data

We will only process special categories of data (also known as sensitive data) where the data subject explicitly consents to such processing or where one of the following conditions apply:

- The processing relates to personal data which has already been made public by the data subject.
- The processing is necessary for the establishment, exercise or defence of legal claims.
- The processing is specifically authorised or required by law.
- The processing is necessary for the purposes of exercising or performing any right, obligation or public function conferred or imposed by law on the JADC in connection with employment, social security, social services or social care.
- The processing is necessary to protect the vital interests of the member or of another natural person where the member is physically or legally incapable of giving consent.
- Further conditions, including limitations, based upon national law related to the processing of genetic data, biometric data or data concerning health.

In any situation where special categories of data are to be processed, prior approval must be obtained from the Data Protection Advisor, and the basis for the processing clearly recorded with the personal data in question. Where special categories of data are being processed, we will adopt additional protection measures.

Children's Data

Children under the age of 13 are unable to consent to the processing of personal data. Consent must be sought from the person who holds parental responsibility over the child. However, it should be noted that where processing is lawful under other grounds, consent need not be obtained from the child or the holder of parental responsibility.

Data Quality

We will adopt all necessary measures to ensure that the personal data we collect, and process is complete and accurate in the first instance and is updated to reflect the current situation of the member. The measures adopted us to ensure data quality include:

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

7 Data Retention

To ensure fair processing, personal data will not be retained by us for longer than necessary in relation to the purposes for which it was originally collected, or for which it was further processed. The length of time for which we need to retain personal data is set out in Appendix A – Data Retention Schedule.

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

For example; when someone leaves the Club and does not renew their membership we would retain their data for a period of 2 years.

8 Data Protection

We will adopt physical, technical, and organisational measures to ensure the security of personal data. This includes the prevention of loss or damage, unauthorised alteration, access or processing, and other risks to which it may be exposed by virtue of human action or the physical or natural environment. A summary of the personal data related security measures is provided below:

- Prevent unauthorised persons from gaining access to data processing systems in which personal data are processed.
- Prevent persons entitled to use a data processing system from accessing personal data beyond their needs and authorisations.

- Ensure that personal data in the course of electronic transmission during transport cannot be read, copied, modified or removed without authorisation.
- Ensure that access logs are in place to establish whether, and by whom, the personal data was entered into, modified on or removed from a data processing system.
- Ensure that personal data is protected against undesired destruction or loss.
- Ensure that personal data collected for different purposes can and is processed separately.
- Ensure that personal data is not kept longer than necessary

JADC has an IT administrator responsible for the security measures outlined above. The only person with administrator rights to the processing system used by the JADC will be the administrator. The administrator will assign permission levels for access, email accounts for new committee members, directors and producers of productions and exchange of accounts for role nominated emails only.

Ex-committee members, directors and producers of productions who no longer use their named email account, the account will be suspended by the administrator and emails in the various boxes will be retained for a period of 2 years, thereafter they will be deleted from the system and the account closed.

9 Data Subject Requests (DSAR)

The Data Protection Advisor will establish a system to enable and facilitate the exercise of data subject rights related to:

- Information access.
- To be informed
- Objection to processing.
- Objection to automated decision-making and profiling.
- Restriction of processing.
- Data portability.
- Data rectification.
- Data erasure.

If a member makes a request relating to any of the rights listed above

Under the Data Protection (Jersey) Law 2018, organisations are required to respond to subject access requests within **four weeks**. Failure to do so is a breach of the Data Protection (Jersey) Law 2018 and could lead to a complaint being made to the Data Protection Regulator.

This policy informs members of the process for supplying information following a request for personal information under the Data Protection (Jersey) Law 2018. Specifically:

- All members need to be aware of their responsibilities to provide information when a data subject access request is received.
- Requests should include the full name, date of birth and address of the person seeking access to their information. To comply with the Data Protection (Jersey) Law 2018,

information relating to the individual must only be disclosed to them or someone with their written consent to receive it.

- No fee can be charged for initial DSAR for all types of records, whether manual or electronic format.

When a subject access request is received from a current or previous member it should **immediately be reported to the IT administrator** who will log and track each request *(all details to be recorded on the JADC Subject Rights log)*. The JADC committee will be informed that a DSAR has been received and is being dealt with. There is no requirement to document the DSAT receipt in the Committee minutes of meeting.

The JADC Chairperson and Secretary will have access to the DSAR log, which will contain details of the request *(date received, by whom, who received it,* personal details of the requestor, identification verification, 'Live' date, Date response is due by, systems checked, who dealt with request, who redacted, who authorised disclosure). This must be kept in confidence.

The IT administrator will need to consider the following before deciding how to respond:

- Requests can be made in any format. All DSARs received by telephone call, verbal request, email, mail, fax, social media, etc. must be processed. (template form is attached at Appendix C but is not mandatory).
- If the requestor is personally known, there is no requirement to request identification documents. If there is reasonable doubt about the identity of the requestor, then the JADC may require further information to verify the requestor's identity. Examples of suitable documents include:
  - Valid Passport
  - Valid Identity Card
  - Valid Driving Licence
  - Proof of address e.g. a named utility bill (no longer than 3 months old)

The JADC will consider each such request in accordance with the Data Protection (Jersey) Law 2018. No administration fee will be charged for considering and/or complying with such a request unless the request is deemed to be repetitive, unnecessary or excessive in nature.

Redaction of data

The IT administrator will gather all the required data from the JADC systems, electronic or paper and create a "Bundle". The JADC Committee, represented by the Chairperson and the Secretary, have the responsibility to issue the data package to the requestor. Before issuing the "Bundle" prepared by the IT administrator, it should be examined and inappropriate data should be redacted. The reason for redaction is to protect the rights and freedoms of others.

This "Bundle" will be reviewed to ensure that it only contains material that is properly disclosable to the individual. There are certain exemptions which may apply to certain information.

The exemptions used will vary, but the main one used will be the identification of third parties. In some circumstances it may not be possible to disclose to the requestor some of their own personal data, without also disclosing data which relates to another individual who can also be identified. This may occur, for example:

- Where another individual gives their opinion about the requestor. An opinion can reveal personal data about the giver of the opinion as well as the person to whom the opinion refers; or
- Where a record contains an account of an event involving both the requestor and another individual.

The Chairperson and Secretary may use an external 3rd party to carry out the redaction exercise if they feel this is appropriate. The redacted "Bundle" will be passed back to the IT administrator, who will arrange for the Chairperson and Secretary to view both bundles (original and redacted) to authorise as Data Controller the disclosure to the requestor.

The IT administrator will retain the original "Bundle" securely together with the redacted "Bundle". Both "Bundles" will be retained for the a period of 1 year after which, subject to agreement of the JADC Committee the "Bundles" will be securely disposed of.

If a request has already been complied with and an identical or similar request is received from the same individual a reasonable fee can be charged for the second request unless a reasonable interval has elapsed.

If a current or previous member is dissatisfied with the way we have dealt with their subject access request, they should be advised to invoke our complaints process. If they are still dissatisfied, they can complain to the Office of the Information Commissioner, Jersey. Full detail below.

10 Law Enforcement Requests & Disclosures

In certain circumstances, it is permitted that personal data be shared without the knowledge or consent of a current or previous member. This is the case where the disclosure of the personal data is necessary for any of the following purposes:

- The prevention or detection of crime.
- The apprehension or prosecution of offenders.

If we process personal data for one of these purposes, then it may apply an exception to the processing rules outlined in this policy but only to the extent that not doing so would be likely to prejudice the case in question. If we receive a request from a court or any regulatory or law enforcement authority for information relating to one of our members, we must immediately notify the Data Protection Advisor.

11 Data Protection Training

Our committee and members that have access to personal data will have their responsibilities under this policy outlined to them as part of their training or induction. In addition, we will provide regular Data Protection training and procedural guidance for our members.

12 Complaints handling

Current and previous members with a complaint about the processing of their personal data, should put forward the matter in writing to the Secretary of the JADC. An investigation of the complaint will be carried out to the extent that is appropriate based on the merits of the specific case. The Secretary will inform the current or previous member of the progress and the outcome of the complaint within a reasonable period. If the issue cannot be resolved through consultation between the current or previous member and the Secretary, then the current or previous member may, at their option, seek redress through mediation, binding arbitration, litigation, or via complaint to the Office of the Information Commissioner, Jersey.

13 Breach Reporting

Any member who suspects that a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data might have occurred, must immediately notify the Chairperson and Secretary of the JADC and provide a description of the circumstances. Notification of the incident can be made via e-mail, by telephone, or in person.

The Chairperson, Secretary and if required, the IT administrator will investigate all reported incidents to confirm whether or not a personal data breach has occurred. If a personal data breach is confirmed, the Chairperson of the committee will follow the data breach notification procedure based on the significance and quantity of the personal data involved. For severe personal data breaches, the committee will coordinate and manage the personal data breach response.

All personal data breaches must be reported immediately to the Chairperson and Secretary of the JADC committee

If a personal data breach occurs and that breach is likely to result in a **risk** to the rights and freedoms of current or previous members (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the **Chairperson and secretary must ensure that they receive specific advice from the JADC Advocate, Advocate Davida Blackmore.** Following that advice, when received in writing, a decision will be made by the JADC committee about the reporting of the Data Breach to the Office of the Information Commissioner, Jersey. This written advice and reporting, if required must be within 72 hours after having become aware of Data Breach.

In the event that a personal data breach is likely to result in a **high risk** to the rights and freedoms of data subjects, the Chairperson and Secretary of the JADC committee must ensure that all affected data subjects are informed of the breach directly and without undue delay.

Data breach notifications shall include the following information:

- The categories and approximate number of members concerned;
- The categories and approximate number of personal data records concerned;
- The name and contact details of our Chairperson and Secretary;
- The likely consequences of the breach;
- Details of the measures taken, or proposed to be taken, by the JADC to address the breach including, where appropriate, measures to mitigate its possible adverse effects.

14 APPROVAL AND REVIEW DETAILS

Approval and Review	Details
Approval Authority	JADC Executive Committee
Data Protection Advisor	Davida Blackmore
Next Review Date	25/01/2021

Approval and Amendment History	
Original Approval Authority and Date	JADC Executive Committee 25/01/2020
Amendment Authority and Date	

Appendix A – Data Retention Schedule:

Data Section	Type of Record	Retention Period		
		Number	Period	Counted from
Club Records	All Club registers		Life of Club	Date of creation of register
	Standard terms and conditions for membership		Life of Club	From creation
Member Accounting Records	Application forms	10	Years	From month of application
	Annual club fees	10	Years	From month of payment
	Statements	10	Years	From month of statement
	Members transaction records	18	Months	From month of transaction
Supplier detail and Accounting Records	Delivery notes	10	Years	From month of delivery
	Invoices	10	Years	From month of invoice
	Statements	10	Years	From month of Statement
Email accounts	for position nominated i.e. President@, Secretary@ etc		Life of the club	It must be noted that no unnecessary data is to be stored in these accounts. Only data relevant to the position.
	Committee name accounts i.e. J.Smith@	2	Years	From date of email
	Director and producers for productions	2	Years	From date of email
Banking records	Bank statements / Reconciliations	6	Years	End of the last club financial year
	Cheques/Bill of exchange and other	6	Years	End of the last club financial year
	Negotiable instruments	6	Years	End of the last club financial year
Health & Safety / Risk records	Health and safety manuals	6	Years	following any updates or amendments
	Minutes of meetings	6	Years	From data minutes formally agreed
	Accident/incident/near miss records	3	Years	from date of entry
	Risk assessments	3	Years	from assessment date
	Examination/Maintenance records	7	Years	From date of completion of any examination or maintenance

	Detail of members exposed to hazardous substance i.e. Asbestos	40	Years	From date of any hazardous material reports
Contracts/ Agreements	Buildings, maintenance, repairs etc.	15	Years	After performance obligation met
Marketing	Consents for direct marketing		Life of valid consent	unless consent is withdrawn
	Register of consent withdrawal		Life of club	This to ensure material is not sent out to member
	Consents for use of information to improve service		Life of valid consent	unless consent is withdrawn
	Newsletter data base		Life of club	unless consent is withdrawn
Insurance Records	Club Liability Certificate	40	Years	From date of expiry
	Renewal Documents and policies	40	Years	Until all claims are settled
	Claims correspondence	3	Years	After claims are settled
Property records - Legal documents	Deeds of Title		Life of Club	Until sold or transferred
	Leases/Licences	15	Years	After expiry
	Listed Building Consents		Life of Club	Until sold or consent expired
	Planning Consents		Life of Club	Until sold
Property records - Project documents for buildings	Specifications/Bills of Quantity	25	Years	
	Tender Documents/Agreements with Contractors & Consultants	10	Years	After project completed
	Surveys & Inspections		Life of Club	
Property records - Reports	Asbestos Inspections	40	Years	

	Architectural; building condition;	25	Years	
	Conservation; site surveys; plans.	25	Years	
	maps & drawings;	25	Years	
Property records - Maintenance records	Maintenance contracts & related files	10	Years	After end of contract
	Maintenance schedules & programmes	10	Years	
	Maintenance log	10	Years	
Information Management	Information Management Policies		Life of Club	
	Retention and Disposal Schedules		Life of Club	
	Procedure Manuals, Guides and Instructions on Management of Records		Life of Club	
	Club visitor sign-in records	5	Years	from last record
	Subject Access requests	1	Year	From date request disclosed
	Subject rights register	6	Years	From completion date
	Original request response bundle	1	Year	From 60 days after disclosure
	Redacted bundle of request response (authorised and sent to requestor)	1	Year	From 60 days after disclosure
	Data Breach Register	6	Years	From date of breach
Information systems records	System Maintenance Log, Quality		Life of Club	
	Control Log		Life of Club	

Appendix B – Data Processing Activity Register:

DP Activity	Purpose	Categories of Personal Data	Categories of Special Data	Categories of Data Subjects	Recipients of Data	Data Volume	Data Format	Data Location	Data Security Measures	Lawful Basis
Members data	Keeping a database of members of the club (past and present – members data kept for 12 months after members lapses)	Name, address, contact details, email address, age and date of birth, theatrical interests, previous stage experience, Profession, membership date and renewal date. DBS checks, any first aid qualification	Medical information (juniors)	Club members Parents of junior club members	Director, Assistant secretary, IT manager, Publicity manager (membership directory supplied to members)	TBC	Electronic (paper membership forms transferred to database) Paper – membership directory	Google G suit iCloud storage, google drive and on mail chimp (email server) No personal data stored on personal devices. Wix.com – membership directory on a secure member only section of the website (in the progress)	Committee members have access to the member data via individual logins (assistant secretary – google drive access, IT manager- google drive and mail chimp access, Publicity manager – google drive and mail chimp access) have edit access.	Data Protection (Jersey) Law 2018 Article 9 – Schedule 2 Pt 1. 1. Consent 2. Contract 3. Legitimate Interest Schedule 2 Pt 2 6. Consent
production	Google account used for all communication with cast and crew (run by director, producers and child liaison officer. This account will be closed following completion of production)	Members names and contact information	N/A	Club members	Director, producer, child liaison officer	TBC	Google drive account for communication with staff	Google drive online servers that contains contact of those involved in the production in order to communicate using this google account.	Google drive security measures. Access via log in. (director – cast list, child medical info if relevant. Producer – cast list, child medical info where relevant. Child liaison officer – child medical info.	Data Protection (Jersey) Law 2018 Article 9 – Schedule 2 Pt 1. 1. Consent 2. Contract 3. Legitimate Interest Schedule 2 Pt 2 6. Consent
marketing	Send marketing communications to contacts	Name, email address	N/A	Normally collected form members (ex-members)	Secretary, assistant Secretary	TBC	Electronic communication	Email server (mail chimp)	Outlook security measures	Data Protection (Jersey) Law 2018 Article 9 – Schedule 2 Pt 1. 1. Consent 2. Contract 3. Legitimate Interest

Appendix C. Subject Access Request Form:

SUBJECT ACCESS REQUEST FORM

If you want us to supply you with a copy of any personal data we hold about you, please complete this form and send it to the address below. You are currently entitled to receive this information under Data Protection (Jersey) Law 2018 (DPJL). We will also provide you with information about any processing of your personal data that is being carried out, the retention periods which apply to your personal data, and any rights to rectification, erasure, or restriction of processing that may exist.

The information you supply in this form will only be used for the purposes of identifying the personal data you are requesting and responding to your request. The Jersey Amature Dramatic Club (JADC) will respond to your request within four-weeks of confirming your identification.

Please send your completed form and proof of identity to:

Secretary
Jersey Amateur Dramatic Club (JADC)
The Barn
La Rue Du Trot,
St Saviour
Jersey
JE2 7JQ

Section 1: Details of the person requesting information

Your full name:	
Your address:	

Your telephone number:	
Your email address:	

Section 2: Are you the data subject?
Please tick the appropriate box.

☐ **YES**: I am the data subject. I am able to provide proof of my identity if so requested by the JADC (see below). Please proceed to Section 4.

☐ **NO**: I am acting on behalf of the data subject. I have enclosed the data subject's written authority and I am able to provide proof of the data subject's identity and my own identity if so requested by the JADC. (see below). Please proceed to Section 3.

To ensure we are releasing data to the right person we may require you to provide us with proof of your identity and of your address. In such instances we will ask you to supply us with a photocopy or scanned image (do not send the originals) of an item listed in 1) together with an item listed in 2):

1) **Proof of Identity.** We accept one of the following: passport, photo driving license, national identity card.
2) **Proof of Address.** We accept one of the following: utility bill, bank statement, credit card statement; current driving license or a recent tax bill, (no more than 3 months old)

If we are not satisfied you are who you claim to be, we reserve the right to refuse to grant your request.

Section 3: Details of the data subject

Your full name:	
Your address:	
Your telephone number:	
Your email address:	

Section 4: What information are you seeking?
Please describe the information you are seeking. Please provide any relevant details you think will help us to identify the information you require.

I am a:

☐ Current Member ☐ Previous Member

☐ Current Committee Member ☐ Previous Committee Member

(please state if you are a current or previous member / committee member. This will assist us to locate any data we hold about you)

……
……
……
……
……
……
……
……
……
……
……
……

Please note we are only obliged to provide you with your personal information. If in so doing that would reveal the identity of any third party, we may decline to provide you with the information requested.

Whilst in most cases you will be provided with your personal information free of charge (subject to exemptions that may apply), we nevertheless reserve the right, in accordance with Article 10 DP(J)L 2018 to charge a fee or refuse the request if it is considered to be "manifestly unfounded or excessive". However, we will make every effort to provide you with a satisfactory form of access or summary of information if suitable.

Section 5: Information about the data collection and processing
If you want information about any of the following, please tick the boxes:

☐ Why we are processing your personal data

☐ To whom your personal data is disclosed

☐ The source of your personal data

Section 6: Disclosure of CCTV images
If the information you seek is in the form of video images captured by our CCTV security cameras, would you be satisfied with viewing these images at the site location? We only keep recorded images from our CCTV systems for 7 days, they are deleted thereafter, unless retained for a lawful purpose.

☐ **YES**

☐ **NO**

Section 7: Declaration
Please note that any attempt to mislead may result in legal action.

I confirm that I have read and understood the terms of this Data Subject Access Request Form and certify that the information given in this application to the JADC is true. I understand that it is necessary for the JADC to confirm my / the data subject's identity and it may be necessary to obtain more detailed information in order to locate the correct personal data.

…….. ……
Signature Date

Attachments:
As requested by the JADC, I am enclosing the following copies as proof of identity and address:

Proof of ID	**Proof of Address (dated within the last 3 months)**
☐ Passport	☐ Utility Bill
☐ Driving Licence	☐ Bank Statement
☐ National ID Card	☐ Credit Card Statement
	☐ Tax Bill