JAMESTON COMMUNITY ASSOCIATION

The Community Hall Jameston SA70 8QG

Data Protection policy

JCA is committed to protecting the rights and privacy of individuals, and to meeting the data protection principles of lawfulness, fairness and transparency. The Data Protection Act 1998 (DPA) and General Data Protection Regulations (GDPR) govern the use of information about people, and set out how to handle it securely and properly.

'Personal data' is any information that can be used to identify a living person either directly or indirectly. It can be held on computers, laptops and mobile devices, or in a manual file and it can include simple details like a name, address or email, as well as other identifiers like minutes of meetings, an IP address, a cookie ID, or a photograph.

Any organisation should only collect, keep or use personal data if they are can show that it meets one or more of a series of legal criteria, which include:

- to serve its group's 'legitimate interests'
- with the explicit consent of the person whose data it is.

JCA uses personal data to build and maintain an accurate record of members, who give their consent to us holding and using their data when they sign up as members.

Organisations that carry out any activities under the regulations have to register with the Information Commissioner's Office and pay an annual fee, but there are exemptions from this requirement and the 2018 *Review of exemptions from paying charges to the Information Commissioner's Office* clarifies that JCA does not have to register.

> *The exemption for not-for-profit organisations … applies to processing which is for the purposes of: establishing or maintaining membership; supporting a not-for-profit body or association, or providing or administering activities for either the members or for those who have regular contact with the organisation.*

JCA is exempt from ICO registration as we hold data solely to maintain an accurate membership list purposes, and for no other purpose. We do not share our list, or use it for marketing, promotion, or in any other way.

Our members also give us permission to hold their data to maintain a current membership list, and they have the option to give us permission to contact them by email or post, with information, updates, and news of forthcoming meetings. The only other personal data that JCA holds is that which is sent to us unsolicited, as contact details in emails or letters.

The JCA remains the data controller for the information held. The trustees and any volunteers are personally responsible for processing and using personal information in accordance with the Data Protection Act and GDPR.

Principles of Data Protection

We ensure that all personal data that it holds will be:

- processed lawfully, fairly and in a transparent manner
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (purpose limitation)
- adequate, relevant and limited to what is necessary (data minimisation)
- accurate and kept up to date (data accuracy)
- kept in a form which permits identification of data subjects for no longer than is necessary (storage limitation)
- processed in a way that ensures appropriate security of the personal data, including protection against accidental or unauthorised access to, or destruction, loss, use, modification, or disclosure of personal data (integrity and confidentiality).

Privacy by design

Privacy by design is an approach that promotes privacy and data protection compliance from the outset. JCA has adopted this approach and, as long as it does not have a negative impact on an individual, privacy settings are set to the most private, by default.

Lawful, fair and transparent

JCA conducts an annual data audit, to ensure that our data processing is lawful, fair and transparent. The audit framework explains where and why we process personal data, and reviews our privacy notices, which are available on our website (www.Jameston CA.co.uk). The privacy notices confirm that:

- the sole reason for us processing personal data is to maintain an accurate and up-to-date membership list, and
- we do not use personal data for any other purpose, unless it is compatible with our original purpose, or we get consent, or we have a clear legal obligation or function.

Data minimisation

We ensure that the personal data we are processing is:

- adequate – sufficient to properly fulfil our stated purpose;
- relevant – has a rational link to that purpose; and
- limited to what is necessary – we do not hold more than we need for that purpose.

Storage limitation

JCA keep members' personal data in a secure file, and we do not keep personal data for longer than is needed to maintain an accurate and up-to-date list of members.

Data accuracy

We ensure that the data we hold is correct and up-to-date, to maintain an accurate and current membership list.

We take all reasonable steps that this is the case, and that nothing is misleading as to any matter of fact. Should we discover that personal data is incorrect or misleading, we take reasonable steps to correct or erase it as soon as possible.

Integrity and confidentiality

The only people with access to our membership list are the trustees with specific responsibility for maintaining it, and the Secretary, who sends out notices to all members.

We use up-to-date computer security measures to ensure that our files are secure, and safe from attack and intrusion.

Rights of individuals

Individuals have the right to access their personal data and we deal with any such requests in line with legal requirements.

The UK GDPR provides the following rights for individuals in relation to their personal data:

- the right to be informed – we do this by making sure our privacy notices are correct and up to date and readily available on our website*, JamestonCA.co.uk*
- the right to access their own data – any request for access goes to the JCA Secretary, who carries out a full search all of our systems before responding to the individual within 30 days, as required by law.
- rectification – we quickly update any personal data which has been identified as inaccurate or incorrect.
- erasure – we will remove any personal data if an individual request this, unless we have another lawful basis which would prevent this
- to restrict processing - where there is a dispute about the accuracy, validity or legality of personal data we hold, an individual has the right to require us to cease processing data for a reasonable period of time, to allow the dispute to be resolved.
- the right to data portability - we will provide an individual with their data in a common and machine-readable electronic format.
- the right to object – complaints or objections to processing personal data are dealt with quickly and accurately.
- rights in relation to automated decision making and profiling – we do not carry out any automated decision making or profiling of any individual.

Data breach

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.

All trustees are able to identify a suspected personal data breach, which could include:

- access by an unauthorised third party to personal data
- deliberate or accidental action (or inaction)
- sending personal data to an incorrect recipient
- computing devices containing personal data being lost or stolen;
- alteration of personal data without permission
- loss of availability of personal data.
- leaving a file on a train

Where a member of staff discovers or suspects a personal data breach, this should be reported to the DPO as soon as possible.

Were there to be a likely risk to individuals' rights and freedoms, JCA would report the personal data breach to the Information Commissioner's Office within 72 hours of being aware of the breach, and also inform the individuals concerned, straightaway.

The JCA Secretary keeps a record of all personal data breaches reported and reports them to a Management Meeting, which identifies and implements appropriate measures and improvements to reduce the risk of reoccurrence.

Operational guidance

emails often contain personal information, and any emails that do, which are no longer required for operational use, should be deleted from the inbox and any "deleted items" box.

If an email (incoming or outgoing) needs to be kept as an official record, save it to an appropriate folder or print and store it securely. If not, delete it.

Phone calls can lead to unauthorised use or disclosure of personal information, so if you receive a phone call asking to check or confirm personal information, remember that the caller may be someone impersonating a person who does have a right of access.

In such a situation, do not give out any personal information, but call them back on a number you know o be accurate, or ask them to write to you for the information.

Laptops and portable devices that hold data containing personal information must be protected with a suitable encryption program (password).

Use **passwords** that are hard to guess, at least six characters long, with both upper and lower-case letters and preferably some numbers.

Always make sure your laptop is locked (password protected) when left unattended, even for short periods, and when travelling in a car, leave it out of sight, preferably in the boot.

Do not give out your password, write it somewhere on your laptop, or keep it written on something stored in the laptop case.

If you have to leave your laptop in a car for a short period, put it in the boot, lock all the doors and set the alarm.

Never leave laptops or portable devices in your vehicle overnight, or leave them unattended in restaurants or bars, or any other venue. And if you are on public transport, keep it with you at all times, do not leave it in a luggage rack or even on the floor alongside you.

Always lock (password protect) your computer or laptop when left unattended.

The data stored should be as little as possible, and restricted to essential files. It must be stored securely and only be accessible to authorised individuals.

If you receive personal data on a disk or memory stick, save the data to the relevant file on the server or laptop, and then return the disk or memory stick (if applicable), or store it safely, or wipe it and dispose of it securely.

Store information for only as long as it is needed or required by statute and will be disposed of appropriately. For financial records this will be up to 7 years and for archival material such as minutes and legal documents it is an indefinite period. Other correspondence and emails will be disposed of when no longer required or when trustees or volunteers retire.

Finally, all personal data held for the organisation must be non-recoverable from any computer which has been passed on/sold to a third party.