St Andrew's *the world's oldest youth club, founded 1866*

Alec Wizard House 12 Old Pye Street Westminster London SW1P 2DG

T 020 7222 6481 E info@standrewsclub.com W www.standrewsclub.com

St Andrew's Club
Information Governance Policy
At 3 September 2019

1. Introduction

1.1 Information is a vital asset, both in terms of the recording of individual members and the efficient management of services and resources.

1.2 It is of paramount importance to ensure that information is effectively and efficiently managed, and that appropriate policies, procedures and management accountability provide a robust governance framework for information management to have a system for handling personal information in a confidential and secure manner to appropriate ethical and quality standards.

2. Definitions

2.1 **Information Governance** is the structures, policies and practices in place to ensure the confidentiality and security of all records, including supporters' and members' records, and to enable the ethical use of them for the benefit of individual supporters and members and the public good.

2.2 **Personal data** under the GDPR (European General Data Protection Regulation 2016/679) mean any information relating to an identified or identifiable natural person.

2.3 **Sensitive personal data** under the GDPR means data consisting of racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation.

3. Scope of the Policy

3.1 The policy applies to all information used by St Andrew's Club, all information systems managed by St Andrew's Club, any individual using information 'owned' by St Andrew's Club and any individual requiring access to information 'owned' by St Andrew's Club.

3.2 This includes, but is not limited to present and historic supporters' information, members' information, Personnel Information, Management Committee Information and Organisational Information, whether as part of structured record systems, either paper or electronic or during transmission or storage of information utilising, e-mail, post or telephone. See also St Andrew's Club Privacy Policy for Supporters and St Andrew's Club - Members' Confidentiality Policy 2019.

3.3 The aims of the policy are to ensure that St Andrew's Club follows the six data protection principles under GDPR so that data is:

1. processed lawfully, fairly and in a transparent manner in relation to individuals;
2. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

3. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
4. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate (having regard to the purposes for which they are processed) are erased or rectified without delay;
5. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
6. processed and stored 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, using appropriate technical or organisational measures.

3.4 The objectives of the policy are to ensure that St Andrew's Club follows the lawful basis of processing personal data under the GDPR, and that this processing satisfies at least one of the following conditions:

1. Consent of the data subject;
2. Necessary for the performance of a contract with the data subject or to take steps preparatory to such a contract;
3. Necessary for compliance with a legal obligation;
4. Necessary to protect the vital interests of a data subject or another person where the data subject is incapable of giving consent e.g. medical emergencies;
5. Necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
6. Necessary for the purposes of legitimate interests.

3.5 The Privacy and Electronic Communications Regulations (PECR) sit alongside the Data Protection Act. They give people specific privacy rights in relation to electronic communications and St Andrew's Club will ensure it complies with the relevant areas the PECR covers:

- Marketing by electronic means, including marketing calls, texts, emails and faxes. PECR applies to us as we market by email;
- The use of cookies or similar technologies that track information about people accessing a website or other electronic service. PECR applies to us as we use cookies on our website. Their use is covered in the website Privacy Policy and visitors are alerted to them by a Cookie Pop Up; Security of public electronic communications services. N/A

- Privacy of customers using communications networks or services as regards traffic and location data, itemised billing, line identification services (eg caller ID and call return), and directory listings. N/A

4. Policy

St Andrew's Club recognises the need for an appropriate balance between openness and confidentiality in the management and use of information. It fully supports the principles of corporate governance and recognises its public accountability as a charity, but equally places importance on the confidentiality of, and the security arrangements to safeguard, both personal information about members, staff, supporters and commercially sensitive information.

5. Consent

Consent is one of the most frequently relied upon condition by St Andrew's Club and the most appropriate lawful basis to process data of supporters' information, members' information, P personnel Information, Management Committee information and organisational information. Since May 25th 2018 when the GDPR came into effect, we are: asking people to positively opt in via a website link to our database, via a website link to our Mailchimp account, or via 1:1 emails/phone calls/in person outlining the different communications options.

- We use clear, plain language that is easy to understand.
- We specify why we want the data and what we're going to do with it.
- We give individual ('granular') options to consent separately to different purposes and types of processing.
- We name our organisation and any third party controllers who will be relying on the consent.
- We tell individuals they can withdraw their consent.
- We ensure that individuals can refuse to consent without detriment.
- We avoid making consent a precondition of a service.

6. Legitimate Interests

Legitimate interests may provide a further lawful basis for processing, and before proceeding St Andrew's Club will always:

- Check that *legitimate interests* is the most appropriate basis.
- Understand our responsibility to protect the individual's interests.
- Conduct a *legitimate interests* assessment (LIA), if necessary, and kept a record of it, to ensure that we can justify our decision.
- Identify the relevant *legitimate interests*.
- Check that the processing is necessary and there is no less intrusive way to achieve the same result.
- Do a balancing test of whether an individual's interests do not override those *legitimate interests* and then be confident that the individual's interests do not override those *legitimate interests*.

- Only use individuals' data in ways they would reasonably expect, unless we have a very good reason.
- Not use people's data in ways they would find intrusive or which could cause them harm, unless we have a very good reason.
- When we process children's data, we take extra care to make sure we protect their interests by insisting on an up-to-date contact details of a responsible adult. We rely on consent from the individual (Senior Club), or responsible adult (Junior Club), as our lawful basis for processing personal data.
- Consider safeguards to reduce the impact (of contacting an individual using legitimate interests) where possible.
- Consider whether we can offer an opt out.
- If our LIA identifies a significant privacy impact, we will consider whether we also need to conduct a DPIA (Data Protection Impact Assessment).
- We will keep our LIA under review as necessary, and repeat it if circumstances change.
- We include information about our l*egitimate interests* in our privacy notice.

7. Accountability and Responsibilities

7.1 The Chief Executive has overall accountability and responsibility for governance, including information governance and is the nominated Data Controller and **Senior Information Risk Owner (SIRO)** of the Management Committee. The Chief Executive will take the strategic lead for information governance and will:

- understand how the strategic business goals of St Andrew's Club may be impacted by information risks;
- act as an advocate for information risk on the Board of Trustees;
- ensure that identified information security threats are followed up and incidents managed.

7.2 The Chief Executive has specific responsibilities in relation to members' information to:

- justify the purpose(s) for using confidential information;
- only use it when absolutely necessary;
- use the minimum information that is required;
- provide access and share information on a strict need-to-know basis;
- ensure everybody understands his or her responsibilities relating to confidentiality;
- understand and comply with the law.

7.3 The Chief Executive also has overall responsibility for any records or information relating to fundraising activity.

7.4 The Chief Executive has overall responsibility for all staff and volunteer records.

7.5 The Office Manager has overall responsibility for all financial, payroll and business operation records such as purchase records and will ensure they are held securely and available for internal or external scrutiny and audit. The Office Manager is the nominated Data Protection Officer.

7.6 The Chief Executive has overall responsibility for all estate, building and statutory related records.

7.7 All the above parties are collectively the Information Asset Owners (IAO) for their defined areas of responsibility. Their principle roles are –

- understand and address risks to the information assets they own;
- provide assurance to the SIRO on the security and use of these assets;
- ensure that any service developments or changes adequately consider information governance and information risk. Wherever there are residual risks specialist advice should be sought;
- ensure that periodical and routine audits, inspections and spot checks are undertaken with regard to the security, quality and completeness of the records within their defined areas of responsibility.

7.8 Any person with a **supervisory role** within the organisation has an operational responsibility to undertake spot checks as agreed with the above Information Risk Owners and for ensuring that persons under their supervision understand and implement their responsibilities as defined in this policy.

7.9 All **Staff and Volunteers** are responsible for the confidentiality, security and appropriate use of any information, whether verbal, written, recorded or electronic, that they will legitimately have access to or that may come into their possession as part of their daily work within St Andrew's Club. These responsibilities are summarised in the Staff Handbook. They should also comply with the Computer Security and Use and the Email Policies best practice.

7.10 **Any Person** who transports or stores any personal data, particularly sensitive personal data is responsible for the safe keeping and confidentiality of that data. All mobile media storage must be fully encrypted. Similarly, any person printing personal data or sensitive personal data is responsible for the safe keeping, use, storage and where appropriate secure disposal of the information.

8. Monitoring

The Information Risk Owners will monitor information risk relative to their own data assets and provide a regular summary of assurance or information risks and actions on-going to the Chief Executive.

9. Review

It is recommended that this policy is reviewed on an annual basis.

Author: Annette Fettes
Date: 3 September 2019