Stalybridge Photographic Club

General Data Protection Regulation

Data Protection Policy

- Policy prepared by: Kev Gamwell (Club Secretary)
- Approved by committee on: 25th April 2018
- Policy to become operational on: 25th May 2018
- Next review date: 24th April 2019

Introduction

Stalybridge Photographic Club (SPC) needs to gather and use certain information about individuals.

The individuals may be members of SPC, visitors to the club such as Judges, Speakers and including potential new members along with other people that SPC has a relationship with or necessity to contact.

This policy describes how personal data will be collected, handled and stored to meet data protection standards and comply with the law.

Why this policy exists

This data protection policy ensures that SPC

- Complies with the law and follows good practice
- Protects the rights of members and club users
- Be open about how it stores, uses and processes personal data of individuals
- Protects itself from a data breach

1. Data protection principles

SPC is committed to processing data in accordance with its responsibilities under the **General Data Protection Regulation (GDPR) (EU) 2016/679 .**

Article 5 of the GDPR requires that personal data shall be:

a. processed lawfully, fairly and in a transparent manner in relation to individuals;

b. 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;

c. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased or rectified without delay;

e. 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; 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

f. 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,

using appropriate technical or organisational measures."

2. General provisions

a. This policy applies to all personal data processed by SPC.

b. The Responsible Persons shall take responsibility for SPC's ongoing compliance with this policy.

c. This policy shall be reviewed at least annually.

d. SPC is understood to be exempt from registering with the Information Commissioner's Office as a non-profit organisation that processes personal data. *(Organisations or individuals who only process personal data for judicial functions, to maintain a public register or for domestic or recreational reasons are exempt.)*

3. Lawful, fair and transparent processing

a. To ensure its processing of data is lawful, fair and transparent, SPC shall maintain a Register of Systems.

b. The Register of Systems shall be reviewed at least annually.

c. Individuals have the right to access their personal data and any such requests made to SPC shall be dealt with in a timely manner.

4. Lawful purposes

a. All data processed by SPC must be done on one of the following lawful bases: consent, contract, legal obligation, vital interests, public task or legitimate interests.

b. SPC shall note the appropriate lawful basis in the Register of Systems.

c. Where consent is relied upon as a lawful basis for processing data, evidence of opt-in explicit consent shall be kept with the personal data.

d. Where communications are sent to individuals based on their consent, the option for the individual to revoke their consent should be clearly available and systems should be in place to ensure such revocation is reflected accurately in SPC's systems.

5. Data minimisation

a. SPC will ensure that all personal data is adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

b. SPC will issue weekly email newsletters and other group emails to members or individuals in order to assist in the running and management of the club and club events. Members have the right to unsubscribe from these emails at any time.

c. SPC will never sell or exchange members personal data to any third party for the purpose of any marketing or profiteering.

d. SPC will only collect names and addresses (physical and email) for club management purposes including an historical record for club archives.

e. SPC members who submit images to club competitions and affiliated competitions e.g. battles or federation competitions will be responsible for the metadata held within those images.

f. SPC utilises a website (static) to serve the club membership and any other community interest. The website does not collect any personal data. The hosting company (34sp) is GDPR compliant.

g. SPC also uses the social media platform Facebook (The Official Stalybridge Photographic Club). The Facebook group is a closed group accessible only to fully paid up members of the club. Facebook is fully compliant with GDPR. No other social media platforms are used by SPC. SPC disassociates itself with any similar named groups on any other platforms.

h. All data held by SPC will be kept on two password protected portable hard drives which will be held by two Officers of the Club. All data will be regularly backed up to ensure the content is up to date. Each of the hard drives will be kept at separate locations in order to maintain a level of security.

6. Accuracy

a. SPC shall take reasonable steps to ensure personal data is accurate.

b. Where necessary for the lawful basis on which data is processed, steps shall be put in place to ensure that personal data is kept up to date.

7. Archiving / removal

a. To ensure that personal data is kept for no longer than necessary, SPC shall put in place an archiving policy for each area in which personal data is processed and review this process annually.

b. The archiving policy shall consider what data should/must be retained, for how long, and why.

8. Security

a. SPC shall ensure that personal data is stored securely using modern software that is kept-up-to-date.

b. Access to personal data shall be limited to personnel who need access and appropriate security should be in place to avoid unauthorised sharing of information.

c. When personal data is deleted this should be done safely and such that the data is irrecoverable.

d. Appropriate back-up and disaster recovery solutions shall be in place.

9. Breach

In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, SPC shall promptly assess the risk to people's rights and freedoms and if appropriate report this breach to the ICO.