Settle Area Swimming Pool

Data Protection Policy

Introduction and purpose

Our data protection policy sets out Settle Area Swimming Pool's (SASP) commitment to protecting personal data in particular. This policy has been updated in the light of the changes in UK Data Protection laws that come into effect on 25 May 2018, namely the Data Protection Act 2018 (DPA), and the General Data Protection Regulation ('GDPR') as it applies in the UK.

Scope of policy

The policy applies to the information processed by SASP, its employees and members of the SASP Trust when conducting the business of SASP, and all temporary and contract workers, and any services delivered by third parties on behalf of SASP.

Policy statements

- SASP will comply with the Principles of the GDPR, and follow the guidance of the Information Commissioner's Office (ICO). A statement of the Data Protection principles (and how SASP complies with these) is reproduced in the Annex at the end of this policy.

- The definition of terms used in this policy follow the definitions in Article 4 of the GDPR.

- SASP will reply to all requests for personal data made by means of a properly completed Subject Access Request (SAR) within a month of receipt.

- SASP will comply with other relevant UK legislation and requirements, when handling personal data, including: Article 8 of the Human Rights Act, the common law duty of confidence, and the Payment Card Industry Data Security Standard (PCI DSS).

- All personal information held by SASP records is regarded as confidential. Information will not normally be disclosed to third parties without the consent of the person concerned. Information may normally be disclosed without consent, to meet statutory requirements; to comply with a court order; to prevent duplication of payments; or where there is a compelling public interest in making the disclosure.

Guidance and further information

This policy is supported by guidance, procedures and advice.

Compliance

All employees of SASP and its Trust are responsible for actively supporting this policy.

The Pool Manager must ensure that:

- employees are aware of this policy and are sufficiently trained in the handling of information.

- there are appropriate procedures in place to ensure that this policy is complied with.

SASP has appointed a Data Protection Officer (DPO), who is responsible for supporting SASP's compliance with this policy, in accordance with Article 39 of the GDPR. In addition, the DPO will:

- Ensure that replies to requests for personal data (SARs) are dealt with in accordance with the law;

- Check and monitor employee compliance on a routine basis;

- Provide general advice, and awareness where necessary, and supporting the management of incidents;

- Report to the manager and Trust as appropriate.

Any failure to comply with this policy may result in disciplinary action, which may lead to dismissal, and/or criminal proceedings.

Review

This policy has been approved by the Trust and will be reviewed at least annually.

Dated: 20 July 2018

Annex

How the SASP complies with the Data Protection Principles

The Data Protection Principles (Article 5, GDPR)

1. Personal data shall be processed lawfully and fairly and in a transparent manner; individuals who provide SASP with their personal data will be informed of SASP's policy on handling personal data by means of a Privacy Notice, which will provide explanatory information about the reasons for the collection of personal data, how the data will be used, and how to obtain a copy of the data.
2. Personal data shall be collected only for specified, explicit and legitimate purposes, and shall not be further processed in a manner that is incompatible with that purpose or those purposes; SASP will only process personal data for the purpose(s) which the data subject was previously informed of and it will not be used for any other purpose that is incompatible with the original purpose(s).
3. Personal data shall be adequate, relevant and limited to what is necessary in relation to the purpose or purposes for which they are processed; SASP will ensure that only the minimum personal data necessary for the purpose is processed and will not collect or hold data on the basis that it might be useful in the future without having a legitimate business reason for how it will be used in the present.
4. Personal data shall be accurate and, where necessary, kept up to date; Processes will be in place to maintain the accuracy of data entry at the point data is first collected by SASP, and to accurately amend, erase, rectify, update or correct personal data.
5. Personal data processed for any purpose or purposes shall not be kept in a form which permits identification of data subjects for longer than is necessary for that purpose or those purposes; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest. SASP must ensure that personal data is securely destroyed once the purpose(s) for processing the personal data has come to an end, and there is no legal requirement or valid business reason for its continued retention.
6. 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, using appropriate technical or organisational measures ('integrity and confidentiality'). SASP will use standard contractual clauses for data protection to be used in any circumstances where processing of personal data on behalf of SASP is carried out by a service provider or other third party. The Data Protection Officer must be consulted in the early stages of any project or proposed change to a business process that has implications for the processing of personal data. All employees must report any incident, or potential incident, likely to result in unauthorised disclosure, damage, destruction or loss of personal data directly to the manager and the Data Protection Officer.

7. SASP is responsible for, and will be able to demonstrate compliance with 1-6 above.