Birtley Community Aquatic Centre
Data Protection/Privacy/GDPR Policy and Guidelines

Version: 1.0

Revision Date: March 2025

Next Review Date: March 2026

1. Introduction

Birtley Community Pool is committed to protecting the personal data of its employees, members, and other stakeholders. This document outlines the procedures and practices in place to ensure that personal data is handled securely and in compliance with legal requirements.

2. Purpose

The purpose of these Data Protection Guidelines is to outline the principles and procedures Birtley Community Pool will follow to ensure the privacy and protection of personal data in compliance with applicable data protection laws, including the General Data Protection Regulation (GDPR). These guidelines are designed to protect the rights of individuals whose personal data is collected, stored, processed, and used by Birtley Community Pool, ensuring that their data is handled lawfully, fairly, and transparently.

These guidelines aim to:

- Safeguard the personal data of employees, members, and other stakeholders.
- Ensure that personal data is collected and processed for legitimate purposes only.
- Maintain the security and integrity of personal data.
- Provide clear instructions to staff, volunteers, and trustees on their responsibilities regarding data protection.
- Outline the rights of individuals regarding their personal data and how these rights can be exercised.

3. Scope

These Data Protection Guidelines apply to all personal data collected, stored, processed, and used by Birtley Community Pool, regardless of format (electronic, paper-based, etc.). The guidelines cover the activities of all staff, volunteers, trustees, and any other individuals who have access to personal data under the control of Birtley Community Pool.

Specifically, the guidelines apply to:

- All personal data related to employees, members, customers, suppliers, and other stakeholders.
- The collection, use, storage, and disposal of personal data across all systems, databases, and physical records.
- Data protection practices related to digital systems, physical files, communications, and marketing activities.
- The transfer of personal data to third parties, ensuring that such transfers comply with legal requirements and are conducted securely.
- The rights of individuals regarding their personal data, including access, correction, deletion, and restriction requests.
- The management of data breaches, ensuring timely reporting and appropriate response actions.

The guidelines are mandatory for all relevant personnel at Birtley Community Pool and are integral to the organisation’s commitment to data protection and privacy.

4. Definition of Personal Data

Personal Data is defined as any information that relates to an identified or identifiable living individual. This includes:

- Name and Surname
- Date of Birth
- Home Address
- Phone Number
- Email Address
- Financial Details
- Identifiable images of an individual, including membership card photos, CCTV, and marketing images
- Any information about a person’s health, medical needs, social care needs, or criminal convictions (classified as ‘special category’ data)

5. Recording Personal Data

When recording personal information, such as setting up a membership or swimming lessons contract, only the necessary information required to provide the service should be requested. All relevant fields must be appropriately completed within our database systems.

Employees must inform individuals why their information is being recorded and ensure that they consent to us holding that data, especially when it includes ‘special category’ data.

- It is essential to inform individuals of the circumstances under which they may be contacted and obtain their consent for such communication. This includes communication via telephone, SMS, or email for direct marketing or market research purposes.
- When using personal data for specific purposes, such as marketing, explicit consent must be obtained. If an individual withdraws consent, this must be honored, and the relevant data or images destroyed immediately.

6. Storing Personal Data

All personal data is stored securely within the appropriate password-protected, encrypted database.

- Databases holding personal data is only accessed from devices owned by and kept at Birtley Community Pool, unless prior agreement has been made for remote access.
- Devices must be securely locked away overnight, and reception desks should not be left unattended while databases are open.
- Any written/printed documents containing personal data must be securely stored and destroyed as soon as possible after being uploaded electronically.
- Passwords should be of high security and only shared with authorised personnel. Staff members must log out of shared devices at the end of each session, and the reception file containing system passwords should be securely locked in the safe at the end of each day.

7. Transferring Personal Data

In exceptional circumstances where personal data needs to be held on a personal device or data storage/transportation device, it must be password-protected and stored in an encrypted folder. It should be deleted once the transfer is complete.

- Personal information should only be sent via email in exceptional circumstances. When necessary, it must be sent from a @birtleycommunitypool email address, in an encrypted file, with the password sent in a separate email.

8. Using Personal Data

Staff, volunteers, and trustees may only access and use personal data in relation to the individual's involvement with the pool and for the purposes agreed upon by the individual.

- Personal data cannot be used for marketing purposes without explicit consent. Any misuse of personal data will be addressed through the disciplinary procedure.
- Personal information must not be shared with other members of the public. Information may only be shared with relevant third parties with the individual's explicit permission or where there is a legal requirement to do so.

9. Deleting Personal Data

Personal information must only be retained for as long as necessary, typically for six years after the individual ceases to receive services, in compliance with tax law. Dormant member data will be archived annually, retaining only the basic necessary information.

- Securely delete or destroy personal information, including deleting emails from electronic folders, cross-shredding paper records, and permanently deleting electronic files and records.

10. People’s Rights Relating to Their Data

Under GDPR, individuals have the right to:

- Request access to the information held about them (Subject Access Request)
- Request corrections, copies of their personal data, or restrictions on its use
- Request the deletion of all or part of the information held about them

Requests for data correction can be completed upon verification, while other requests should be directed to the board of trustees for consideration. BCAC is required by law to respond within 30 days.

11. Running Reports

When running reports, BCAC employees should use the membership/account number of the individual, which contains no personally identifiable information. Only data fields required for the report's purpose should be included.

12. CCTV

Third-party requests for CCTV footage, including from the Police, must comply with legal requirements. Footage may only be shared:

- In an immediate emergency
- Where there is a legal requirement, such as a warrant
- With written requests, including the legal basis for sharing and, if relevant, a crime reference number

Approval from the Chair is required before sharing.

13. Management of Data Breaches

Any breach of this policy, including loss/theft of personal data, must be reported to the Business Support Officer and documented through an incident form.

- The Business Support Officer will determine if the breach needs to be reported to the Information Commissioner’s Office.
- Breaches will be investigated by two board members, which could result in actions to improve practices or disciplinary proceedings where misconduct is identified.

14. Review and Monitoring

This policy will be reviewed annually or in response to any changes in relevant laws or regulations. Any updates will be communicated to all employees.

15. Contact Information

For more information or to discuss data protection issues, please contact:

Amber Barry
Business Support Officer, Birtley Community Pool
Amber.Barry@birtleycommunitypool.org.uk

Lewis Herbertson

Senior Operations Manager, Birtley Community Pool

Lewis.Herbertson@birtleycommunitypool.org.uk

16. Approval

This policy was approved by the Board of Trustees of Birtley Community Pool on 06/03/2025.

Signatories:

Yvonne Probert
Chairperson, Birtley Community Pool Board of Trustees

Tracy Green
HR Trustee, Birtley Community Pool Board of Trustees