

## Confidentiality Policy

### Introduction

This policy has been written to ensure that all staff, volunteers and members understand the Swim England East Region requirements in relation to the disclosure of personal data and confidential information.

Employees and volunteers will regularly receive, and handle, personal and private information about members, clubs, and other partners. We want to make sure that this information is well-protected. It is essential that we protect such information particularly as there are legal requirements to protect sensitive data.

This policy affects all employees, volunteers including board members, discipline managers, committee members, officers, the volunteer workforce at regional events, and consultants carrying out a role for Swim England East Region, any of whom may have access to confidential information.

### Policy elements

Confidential and proprietary information is secret, valuable, expensive and/or easily replicated. Employees and volunteers may have various levels of authorised access to confidential information. Common examples of confidential information are:

- Unpublished financial information
- Data from members (including date of births, email addresses, medical information, DBS checks, home club, phone numbers, email addresses)
- Data from volunteers (medical information, email addresses, phone numbers, DBS checks, home club, and qualifications)
- Data from partners (names, bank details, and email addresses)
- Data entrusted to Swim England East Region (SEER) by external parties (membership database, course registers, entries, distribution lists, and rankings)
- Documents and processes explicitly marked as 'confidential'
- Unpublished discussions, budgets, plans and information marked as 'confidential'

### What employees and volunteers must do:

- Lock or secure confidential information at all times
- Shred confidential documents when they're no longer needed (please refer to the Retention and Disposal Policy)
- Only disclose information to other employees and SEER volunteers when it's necessary and authorised

### What employees and SEER Volunteers mustn't do:

- Use confidential information for any personal benefit or profit
- Disclose confidential information to anyone outside of our organisation
- Replicate confidential documents and files and store them on insecure/ non regionally owned devices unless authorised to do so
- When employees and volunteers stop working for SEER, they're obliged to return all confidential files.

### **Confidentiality Measures**

SEER will take measures to ensure that confidential information is well protected. We will store historical paper documents at the Regional Office which is fitted with an alarm, and has both lock and key code to access. Staff laptops are password encrypted, and documents are solely stored on the encrypted hard drive, regularly backed up on the secure Swim England servers or the Swim England server.

We will provide all existing and newly appointed employees, and SEER volunteers, with a copy of this policy and ask them to sign Non-Disclosure Agreements (NDAs).

### **Exceptions**

Confidential information may occasionally have to be disclosed for legitimate reasons, for example, if a regulatory body requests it as part of an investigation or audit.

### **Disciplinary Consequences**

Employees and SEER volunteers who breach our Confidentiality Policy will face disciplinary and, possibly, legal action.

We will investigate any breach of this Policy and reserve the right to terminate the position of any employee or volunteer who wilfully, or regularly breaches, our Confidentiality Policy for personal profit. We may also have to act upon any unintentional breach of this policy, depending on its frequency and seriousness.

This policy is binding even after separation of employment and ceasing of a volunteer role.

End