Blyth Lifeguard & Swimming Club

GDPR Policy

Introduction

The General Data Protection Regulation (GDPR) is a legal framework that sets guidelines for the collection and processing of personal information from individuals who live in the European Union (EU). GDPR came into force in the UK in May 2018 dramatically changing the way businesses and charities handle and use personal information. Information in this document sets out how we as an organisation should interpret the regulations to ensure we comply with the legislation. Breaches in GDPR regulations place the onus on the organisation to report its self; therefore we need to ensure that we adopt a strict policy that everyone can follow limiting the possibility of any breach.

What is classed as confidential data

Confidential or personal data, for our purposes, means information about a living individual who could be identified from that data, either on its own or when combined with other information. GDPR specifically defines personal data as “any information relating to an identified or identifiable natural person”. This therefore covers the majority of data we need to hold as a club including name, DOB, address, phone numbers, emails and registration numbers (ASA, RLSS, Surf, etc.). Information including racial or ethnic origin, religious beliefs and sexual orientation etc. are classified as sensitive and should also be protected.

GDPR Summary

GDPR is about knowing what you have, knowing what you are doing with it, knowing where it is stored, knowing who has access to it, and knowing how you are safeguarding it.
You have to know all of this, and you have to document all of this. Some of this documentation will be internal, and some of it, such as your privacy information notices, will be public.
In the event of a privacy concern or a data breach, the national data protection regulator (the ICO) will ask to see your documentation.

GDPR Consent

Under GDPR, consent is everything. In most circumstances, data collection and processing must be done with the consent of the people that data is about. Consent must be explicitly gained, be specific, be optional and can’t be implied. For minors consent must be obtained by their parent/guardian and any correspondence with minors should be through letters handed out or through emails via their parents/guardians.

What is classified as a breach

A breach might involve someone outside your organisation viewing, using or stealing personal data. But a breach would also occur if someone within your organisation accessed personal data without authorisation, accidentally deleted or altered personal data or shared personal data with people inside or outside of your organisation without consent or reason.

Consequences of non-compliance

GDPR does have teeth. There are two levels of fines for data protection breaches or actionable poor practice. Level 1 fines can be imposed for up to €10,000,000, and level 2 fines can be imposed for up to €20,000,000.

What we need to do

- Create an inventory of all the data we hold, both online and offline, internal and external;
- Document and justify the purpose and use of the data we hold;
- Designate approved super users who can access this data for the management of the club;
- Designate approved super users who can access transmit data to external parties where necessary;
- Identify approved users who can hold this data for use in day to day activities of the club;
- Continually review our privacy information notices across all areas;
- Continually review consent processes across all areas.

What it means for us

Data collected should be in a safe, controlled environment with access limited to people that need it. Where possible no data should be written down or printed when viewing it online is available, if that information is lost we have breached.

We should **avoid at all costs** asking for information in a public forum which can be viewed by other people. Where possible we should record all information we need in the online membership database and access it through there when we need it.

If we are emailing people, this is allowed under GDPR as long as it is to an email address provided by a member for a specific purpose (not marketing), we must ensure we use the bcc (blind carbon copy) option so email address aren't shared with other members. Carbon copy (cc) may be permitted for Executive Committee member correspondence purposes with prior permission of recipients.

We must monitor access to personal records within the online system and query any anomalies.

We should never share information about members with any external person or organisation without their consent (signing up to competitions or joining ASA and Surf is allowed as they have consented to join these organisations) unless it is deemed there is a safeguarding, criminal or justifiable reason to do so.

Any data printed for a specific purpose e.g. Emergency Contact information should be used for its intended purpose only and once that purpose has been met it should be destroyed.

In summary

GDPR is in place to ensure organisations take steps to ensure that data held about an individual is safe, stored for a reason and never used without reason or consent.

A lot of the GDPR issues come down to common sense; if you think there is an issue with a process or a better way to do it there probably is. You must report any queries or concerns to the Executive Committee immediately. Failure to act is failure to protect.

We must continually be reviewing and updating policies to ensure we are unimpeachable when it comes to data security.
There will be times that data is needed in a hard copy (paper based) but we need to limit these where possible and ensure they are destroyed appropriately as soon as possible.
If you have data or are viewing data you don't need to you are potentially breaching GDPR.