Clare Bridge Club
General Data Protection Regulations Policy

Introduction

Clare Bridge Club needs to gather and use certain information about individuals who are members of the Club and/or who attend events run by Clare Bridge Club

This policy describes how this personal data must be collected, handled and stored to comply with current Data Protection legislation, and to meet the Club's standards.

Why this policy exists

This data protection policy ensures that Clare Bridge Club

- Complies with data protection legislation and follow good practice
- Protects the rights of its members and guests
- Is open about how it stores and processes individuals' data
- Protects itself from the risks of a data breach.

Data protection legislation

The General Data Protection Regulations (GDPR) 2018 describe how organisations — including Clare Bridge Club — must collect, handle and store personal information.

These rules apply regardless of whether data is stored electronically, on paper or on other materials.

There must be a lawful basis for processing personal information. Clare Bridge Club collects personal data that is necessary for the purposes of its legitimate interests as a membership organisation and participant in an internationally recognised and regulated competitive mind sport.

To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The GDPR provides the following rights for individuals:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling

The GDPR is underpinned by six important principles. These say that personal data must:

1. Be processed fairly and lawfully and in a transparent manner in relation to individuals;
2. Be obtained only for specific, explicit and legitimate purposes;
3. Be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
4. Be accurate and kept up to date; every reasonable step must be taken to ensure that inaccurate personal data are erased or rectified without delay;
5. Not be held for any longer than necessary;

6. 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

Special category data includes information about race, ethnic origin, politics, religion, genetics, health, biometrics, sexual orientation. This is categorised as more sensitive information, and if collected, needs more protection. It puts individuals at risk of discrimination, so there must be an additional lawful basis and conditions for processing this information. Clare Bridge Club does not collect this information.

Criminal offence data - To process personal data about criminal convictions or offences, there must be a lawful basis under Article 6 and either legal authority or official authority for the processing under Article 10. Clare Bridge Club does not collect this information.

People, Risks and Responsibilities:

Policy scope

This policy applies to:

- Clare Bridge Club
- Any Officer of Clare Bridge Club
- All Committee members, event organisers, scorers and directors for Clare Bridge Club

It applies to all data that Clare Bridge Club holds relating to identifiable individuals. This can include:

- Contact information
- EBU membership numbers
- Disclosure and Barring Service (DBS) checks done with the member's knowledge and permission
- Scorer and director roles
- Committee membership
- Teaching qualifications

Data protection risks

This policy helps to protect Clare Bridge Club from some very real data security risks, including:

- Breaches of confidentiality**:** For instance, information being given out inappropriately.
- Failing to offer choice: For instance, all individuals should be free to choose how the Club uses data relating to them.

Responsibilities

Under the GDPR Clare Bridge Club does not have a statutory requirement to have a Data Protection Officer. Clare Bridge Club will appoint a Committee member, known as the GDPR Officer, to be responsible for ensuring that the Club discharges its obligations under the GDPR.

Each individual who handles personal data for Clare Bridge Club has responsibility for ensuring that data is collected, stored and handled appropriately.

However, the following people have key areas of responsibility:

- The Chairman must ensure at each AGM the continuity of the role of the GDPR Officer
- The Membership Secretary must ensure that all membership records held in paper format must be stored safely in a way that complies with GPDR, taking advice as necessary from the GDPR Officer
- The Committee Member known as the GDPR Officer has responsibility for ensuring that the Club is compliant with GDPR. The GDPR Officer is responsible for:
    - Keeping the Committee updated about data protection responsibilities, risks and issues.
    - Reviewing all data protection procedures annually
    - Ensuring that all club members/officials who have access to personal data have signed the guidance note and signature panel to confirm that they understand their responsibilities under GDPR
    - Ensuring that all passwords for electronic storage are changed at least annually (including for the EBU, Bridgewebs, Bridgemates, Cloud storage). This should be completed immediately following the Annual General Meeting of the Club each year when Committee members and Club Officers may change.
    - Arranging data protection training and advice for the people covered by this policy.
    - Handling data protection questions from Committee or Club members
    - Dealing with requests from individuals to see the data Clare Bridge Club holds about them (also called 'subject access requests').
    - Checking and approving any contracts or agreements with third parties that may handle the Club's personal data.

General Guidelines:

- The only people able to access data covered by this policy should be those who need it for the legitimate running of the Club and its events.
- Personal data should not be shared informally with anyone except with the express consent of the person to whom the data relates
- Clare Bridge Club will provide training to relevant members regarding their responsibilities when handling data.
- Members of Clare Bridge Club should keep all data secure, by taking sensible precautions and following the guidelines below.
- Members of Clare Bridge Club should not hold any data on personal devices that is not password protected. In particular, strong passwords must be used and they should never be shared.
- Personal data should not be disclosed to unauthorised people, either within the Club or externally.
- Data should be regularly reviewed and updated. If it is found to be out of date or if it is no longer required, it should be deleted and disposed of.
- Members should request help from the GDPR Officer if they are unsure about any aspect of data protection.

Clare Bridge Club
General Data Protection Regulations Policy

Data Storage:

When data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

- Data should be protected by strong passwords that are changed annually as a minimum and never shared.
- If data is stored on removable media (like a CD or DVD), these should be kept locked away securely when not being used.
- Data should only be stored on designated drives and servers, and should only be uploaded to an approved cloud computing service.
- All servers and computers containing data should be protected by approved security software and a firewall.

When data is stored on paper, it should be kept in a secure place where unauthorised people cannot see it. These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper or files should be kept in desk drawers, filing cabinets, cupboards or shelves. Any items stored on a shelf are less secure.
- Club members should make sure paper and printouts are not left where unauthorised people could see them.
- Data printouts should be shredded and disposed of securely when no longer required.

Data Accuracy:

GDPR requires Clare Bridge Club to take reasonable steps to ensure data is kept accurate and up to date.

It is the responsibility of all members of the Club to take reasonable steps to ensure data is kept as accurate and up to date as possible.

- Data will be held in as few places as necessary.
- Clare Bridge Club will make it easy for data subjects to update the information that the Club holds about them, by responding quickly to email or telephone correction.
- Data should be updated as inaccuracies are discovered. For instance, if a member can no longer be reached on their stored telephone number, it should be removed from the database.

Data Retention:

Personal data will only be stored while a person is a current and an active member of the Club. When individuals leave the Club, discontinue their subscriptions, or in the event of their death, their data will be deleted completely from all Club databases at the earliest possible opportunity, but as a maximum within four months. Should an individual subsequently decided to rejoin the Club, then a full membership application must be completed again.

Subject Access Requests:

All individuals who are the subject of personal data held by Clare Bridge Club have the right to:

- Confirmation that the Club is processing their personal data

- A copy of their personal data
- The purposes of the Club's processing;
- The categories of personal data concerned;
- The recipients or categories of recipient the Partnership discloses the personal data to;
- The retention period for storing the personal data or, where this is not possible, the criteria for determining how long it will be stored;
- The existence of their right to request rectification, erasure or restriction or to object to such processing;
- The right to lodge a complaint with the ICO or another supervisory authority;
- Information about the source of the data, where it was not obtained directly from the individual;
- The existence of automated decision-making (including profiling); and

If any individual contacts the Club requesting this information, this is called a "subject access request".

Subject access requests from individuals should be made in writing or by email to the GDPR Officer or the Chairman.

Proof of identity may be required before releasing the information; once identity has been verified the information Clare Bridge Club holds will be provided within 30 days, free of charge. However, requests excessive in nature or repetitive requests may be subject to a fee.

Data Breach:

A personal data breach is a breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access, to personal data. A breach can include:

- Access by an unauthorised third party
- Deliberate or accidental action (or inaction) by a controller or processor (eg Clare Bridge Club)
- Sending personal data to the incorrect recipient
- Computing devices containing personal data being lost or stolen
- Alteration of personal data without permission
- Loss of availability of personal data; for example, by corruption and accidental lost or destruction

All data breaches must be reported to the GDPR Officer and a record of data breaches must be kept, regardless of whether or not they need to be reported to the Information Commissioner's Office (ICO). The GDPR Officer will be responsible for recording such breaches and discerning whether the breach needs to be reported to the (ICO)

Certain types of personal data breach must be reported to the Information Commission within 72 hours of becoming aware of a breach, where feasible. If the breach has a high risk of adversely affect an individual's rights and freedoms then the individual(s) in question must also be informed.

The GDPR Officer will be responsible for informing the English Bridge Union (EBU) of any breach to ensure that the Club has adequate support and legal advice, and also for informing the Club's insurance provider to ensure that the Club is adequately protected in the event of a claim being made against it or the Club being fined by the ICO.

There are significant fines for failing to notify a breach when required, so all data breaches, no matter how small, should be reported to the GPDR Officer.

Providing Information:

Clare Bridge Club aims to ensure that individuals are aware that their data is being processed, and that they understand:

- How the data is being used
- How to exercise their rights

To these ends, the Club has a privacy notice, setting out how data relating to individuals is used by the Club.

The Club's Privacy Notice is available on request, and there is also a copy of this available on the website.

Signed Sarah Farr on behalf of Club)

Print Sarah Farr

Date 22 June 2018

Role Chairman