KINSALE GOLF CLUB
DATA PROTECTION POLICY

Contents

Policy Statement

Kinsale Golf Club has responsibility to maintain high standards of confidentiality for safeguarding information about its members, employees, suppliers, visitors and others with whom the Club communicates and interacts.

During the course of the Club's activities the Club may collect, store and process personal information and the Club recognises the need to treat this data in an appropriate and lawful manner. The Club is committed to complying with its obligations in respect of all personal data held.
The types of information the Club may be required to handle include details of current, past and prospective Members, Employees, Suppliers and Visitors and others with whom the Club communicates and interacts. The information, which may be held on paper, on computer or other media, is subject to certain legal safeguards specified in the DATA PROTECTION ACTS 1988/2003 and other regulations. The Acts impose restrictions on how the Club may collect and process the data. This policy is required to be put in place by the Club by operation of law.

The Club is committed to complying at all times with the Data Protection Acts 1988 - 2003, and, without prejudice to the generality of the foregoing, the eight primary rules of Data Protection, the Guidelines issued by the Office of Data Protection including the Data Protection in the Charity and Voluntary Sector Guidelines, the Personal Data Security Breach Code of Practice as approved by the Data Protection Commissioner under Section 13 (2) (b) of the Data Protection Acts, 1988 and 2003, the published decisions of the Office of Data Protection in Ireland and other binding codes and decisions of the Office of Data Protection as well as the spirit and intent of the aforementioned Acts and Regulations.

Purpose and Scope of the Policy

This policy sets out Club Rules on data protection and the legal conditions that must be satisfied in relation to the collecting, obtaining, handling, storage, transportation and destruction of personal and sensitive information.

If any Member or Employee considers that this policy has not been followed in respect of personal data about themselves or any third party, they have an obligation to raise it with the Data Controller and or Data Protection Officer in writing setting out the breach alleged.

Definition and Scope of the Policy

• **DATA** is information which is stored electronically, on computer or paper based files filing systems.

• **DATA SUBJECTS** for the purpose of this policy include all living individuals about whom the Club holds data.

• **PERSONAL DATA** means data relating to a living individual which can be factual (such as date of birth or contractual details, rates of pay etc.) or it can be opinion (such as performance appraisal).

• **SENSITIVE PERSONAL INFORMATION** means data about an individual which relates to race, ethnic group, political affiliation, religion, trade union membership, mental or physical health, sexual orientation or criminal record.

• **DATA CONTROLLER** shall be the Club who has primary control, and which is primarily responsible for the safekeeping of the data such as the office staff.

• **DATA PROCESSORS** include authorised employees/members whose work involves using personal data.

• **DATA PROTECTION OFFICER** is the person(s) assigned by the Management Committee to supervise and administer all the Club's Data controls. As this is a Club which is managed on a voluntary basis, involves an extremely large management structure that alters annually and is subject to significant turnover and as it is community based, particular and special care must and will be taken at all times to ensure, as hitherto, that the data is kept and maintained strictly confidential and secure.

Data will be accessible to and only be made available to those persons who necessarily and directly require access to the same for the direct and immediate discharge of their duties and responsibilities and such persons are obliged to maintain strict confidentiality in relation to all personal data in keeping with the Data Protection Legislation. The Club shall take all necessary steps to ensure that, where this involves a large group of persons, such steps and actions as shall be necessary and appropriate, in prior consultation and with the agreement of, with the subjects of the said Personal Data, will be taken to secure such data whether by the creation and composition of such sub groups with whom the said Personal Data is to be shared or communicated to or some other appropriate steps. (Nothing herein shall permit or allow Personal Data to be shared with any person or third person who may, in the opinion of the subject of the Personal Data use the same to bully harass or cause harm to the said Data Subjects).

It is a legal requirement for the club to comply with the **Data Protection** Act's, **1988 - 2003** and / or any further amendments thereto. It is also club policy to ensure that every Member and Employee maintains the confidentiality of any personal data held by the club whatever form.

Data Protection Principles

The Club, within reason, needs to keep certain information about its Members, Employees, Visitors and Suppliers for financial and commercial reasons and to enable it to monitor performance, to ensure legal compliance and for health and safety purposes. To comply with the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. This means that we must comply with the Data Protection Principles set out in the Data Protection Act, 1988 and 2003.

These principles require that Personal Data must be:

(1) Obtained fairly and lawfully and shall not be processed unless certain conditions are met.

(2) All data will be stored in the office of the clubhouse and will not be removed from the clubhouse without the permission of the data protection officer(s).

(3) Obtained for specified and lawful purposes and not further processed in a manner incompatible with that purpose.

(4) Adequate, relevant and not excessive.

(5) Accurate and up to date.

(6) Kept for no longer than necessary.

(7) Processed in accordance with data subjects' rights.

(8) Protected by appropriate security.

(9) Not transferred to a country outside the European Union without adequate protection.

In processing or using any personal information the Club must ensure that it follows these principles at all times.

Data Protection Officer

All enquiries relating to the holding of personal data should be referred in writing to the Data Protection Officer(s) in the first instance.
The Data Protection Officers in Kinsale Golf Club are the Club Hon. Secretary.

Notification of Data Held

You are entitled to know:

(a) What personal information the Club holds about you and the purpose for which it is used.

(b) How to gain access to it.

(c) How it is kept up to date.

(d) What the Club is doing to comply with its obligations under the 1998/2003

Acts. This information is available from the Data Protection Officer.

Individual Responsibility

Authorised Members and Employees are responsible for:

(a) Checking that any information that the Club holds is current and up to date.

(b) Notifying the Club of any changes to information you have provided, for example Changes of address; Bank Account details etc.

(c) Ensuring that all parties are familiar with and following the Club Data Protection Policy.

Data Security

The Club is responsible for:

Ensuring complete and comprehensive compliance with the spirit and the letter of the relevant legislative provisions, Guidelines, Codes of Practice and directives from the Office of Data Protection.

Without prejudice to the generality of the foregoing, the Club is responsible for:

a) Understanding that any breach of the data protection policy, either deliberate or through negligence, may lead to disciplinary action being taken and could in some cases result in a criminal prosecution.

b) Ensuring that any personal data that the Club holds, whether in electronic or paper format, is kept securely.

c) Ensuring that Members, Employees, Contractors and Agents are familiar with and following the Data Protection Policy.

d) Personal information is not disclosed either verbally or in writing, accidentally or otherwise, to any unauthorised third party save as agreed and permitted by law.

e) The putting into place of appropriate procedures and security measures to ensure that all information originally furnished to the Club is used and disclosed only for that limited agreed purpose.

f) Putting into place of appropriate procedures and security measures to ensure that all information obtained by one person or disclosed to one person for one specified purpose shall not be disclosed to, accessed by and / or used for, another purpose, entity and or section within the Club. This will include but not necessarily be limited to providing secure data-holding facilities, file tracking, audit trails, confidentiality agreements etc. To ensure that such unauthorised access, where it might take place, can be tracked and provide a basis for appropriate measures to be taken to deal with it both by the Club and by the Office of Data Protection.

g) If one section or organ of the Club wishes to transfer personal data about its members/employees to another part of the same entity then, prior to so doing and to ensure that it is lawful and permissible, ensure that all of the relevant requirements for a transfer of personal data and information have been met and the consent of the affected Data Subjects obtained.

h) Regular and ongoing assessment of the risks and threats that exist to personal data held by the Club, consultation with all stakeholders within the Club in so far as the data protection Acts as amended are concerned.

Golf Ireland

The Club is affiliated to Golf Ireland. Golf Ireland operate and maintain the details of the handicap of members and for this purpose allocates each individual member of the Club a unique personal identifier number (your unique "Club Membership No."). The system has been designed by Golf Ireland to provide members of Clubs affiliated to Golf Ireland, including Kinsale Golf Club, with enhanced membership services free of charge.

The purposes for which Golf Ireland may use the data are as follows:
1. Golf Ireland may use your details to communicate directly with the people who play the sport in Ireland, to provide them with information and other benefits relating to their membership; and
2. The provision of a handicap system for all individual members of affiliated Clubs and the wider golf community through the introduction of the Club Membership Number. You agree that the Club and other Golf Ireland affiliated Clubs at which you may play in competition may provide your name, address, phone number, email address, membership no., gender, date of birth, your card number and your results history to Golf Ireland for the purposes of operating the data base system. The Club agrees to keep your data on the system securely and to only use it for the purposes set out in this notice.

Your handicap details and membership number are displayed in the locker room area of the Clubhouse. Under the Data Protection Acts 1988 and 2003, as amended, you are entitled to write to Golf Ireland at their address or email to request a copy of your personal data which Golf Ireland holds. Similarly, with 'BRS' which operates the club reservation system. (www.brs.com). Should inaccuracies exist in your personal data held by Golf Ireland or BRS, you are entitled to request that they amend or erase it.

Except where required by law to do so, the Club will never provide your personal data to any third party except to your Club or to a competition organiser for the purposes of confirming your details where you enter into a competition using your name and/or your Golf Ireland number. Unless you specifically request the Club Office to do otherwise, it will provide your telephone number and email address to other members for the purposes of arranging matches, changing playing times etc. Other personal information will not be provided directly to other members without your agreement.

The Eight Rules of Data Protection

You must...

1) Obtain and process information fairly.
2) The data must be kept for a specified, lawful purpose.
3) The data should be used and disclosed only for the specified purpose.
4) The data must be kept safe and secure.
5) The data must be up to date, accurate and complete.
6) The data must be relevant, adequate but not excessive.
7) The date must be retained for no longer than is necessary.
8) A copy of the data must be made available to the data subject, on request.

See Appendix 1 - Eight Rules of Data Protection - Comprehensive

Transferring Personal Data Abroad

An area of concern for many data controllers are the requirements necessary for the transfer of data abroad. There are special conditions that have to be met before transferring personal data outside the European Economic Area (all EU countries plus Norway, Iceland and Liechtenstein), where the importing country does not have an EU approved level of data protection law. This is termed a finding of adequacy. In such a case, one of the following conditions must be met if a transfer is to take place. Either the transfer must be:

- Consented to by the data subject; or
- Required or authorised under an enactment, convention or other instrument imposing an international obligation on this state; or
- Necessary for the performance of a contract between the data controller and the data subject; or
- Necessary for the taking of steps at the request of the data subject with a view to his or her entering into a contract with the data controller; or
- Necessary for the conclusion of a contract between the data controller and a third party, that is entered into at the request of the data subject and is in the interests of the data subject, or for the performance of such a contract; or
- Necessary for the purpose of obtaining legal advice; or
- Necessary to urgently prevent injury or damage to the health of a data subject; or
- Part of the personal data held on a public register; or
- Authorised by the data protection commissioner, which is normally the approval of a contract which is based on EU model contracts or the transfer is by a US company which is certified as what is known as safe harbour compliant.[1]

As the legislation on the transfer of data abroad is complex, where doubt arises, the Club will contact this Office in order to seek guidance on specific cases.

---

[1] This is a certification programme overseen by the US Department of Commerce which allows certain US based companies to self-certify as having an adequate level of data protection that meets US standards and consequently personal data can be transferred without the need for recourse to the EU Model contracts

CCTV

Kinsale Golf Club has: -

- Installed a CCTV system which produces clear images which the relevant bodies can use to investigate crime.
- And these can easily be taken from the system when required.
- Sited cameras so that they provide clear images.
- Positioned the cameras to avoid capturing images of persons not visiting the premises.
- Sited monitors in a position that provides the staff with the security required whilst restricting as far as is practical the ability of the public to see them.
- A limited number of authorised persons that may access the recorded images from the CCTV system, which are securely stored. The recorded images are held for 28 days and with the exception of relevant bodies, images will not be provided to third parties.

What constitutes a breach?

Where an incident gives rise to a risk of unauthorised disclosure, loss, destruction or alteration of personal data, in manual or electronic form, the data controller must give immediate consideration to informing those affected. Such information permits data subjects to consider the consequences for each of them individually and to take appropriate measures. If the data concerned is protected by technological measures which make it unintelligible to any person who is not authorised to access it, the data controller may conclude that there is no risk to the data and therefore no need to inform data subjects. Such a conclusion would only be justified where the technological measures (such as encryption) were of a high standard.

All incidents in which personal data has been put at risk should be reported to the Office of the Data Protection Commissioner as soon as the data controller becomes aware of the incident, except when the full extent and consequences of the incident has been reported without delay directly to the affected data subject(s) and it affects no more than 100 data subjects and it does not include sensitive personal data or personal data of a financial nature. In case of doubt- in particular any doubt related to the adequacy of technological risk-mitigation measures - the data controller should report the incident to the Office of the Data Protection Commissioner. See Appendix 2 - Personal Data Security Breach Report Form.

Policy Review

The policy is to be reviewed on an annual basis or at such time that the Data Protection Act is amended. The Data Protection Commissioner provides extensive information and practical guidance on Data protection on its website www.dataprotection.ie and Kinsale Golf Club will continue to inform itself further of its obligations by reviewing this site.

Basic Data Protection Checklist

- Are the individuals whose data the Club collect aware of its identity?
- Has the Club told the data subject what use you make of his/her data?
- Are the disclosures the Club makes of that data legitimate ones?
- Does the Club have appropriate security measures in place both internally and externally to ensure all access to data is appropriate?
- Does the Club have appropriate procedures in place to ensure that each data item is kept up-to-date?
- Does the Club have a defined policy on retention periods for all items of personal data?
- Does the Club have a data protection policy in place?

- Does the Club have procedures for handling access requests from individuals?
- Is the Club clear on whether or not you should be registered?
- Is the Club's staff appropriately trained in data protection?
- Does the Club regularly review and audit the data which you hold and the manner in which they are processed?

Appendix 1 - Eight Rules of Data Protection – Comprehensive

1. Obtain and process information fairly

To fairly obtain data, the data subject must, at the time the personal data is being collected, be made aware of: -

- The name of the data controller.
- The purpose in collecting the data.
- The identity of any representative nominated for the purposes of the acts.
- The persons or categories of persons to whom the data may be disclosed.
- Whether replies to questions asked are obligatory and the consequences of not providing replies to those questions.
- The existence of the right of access to their personal data.
- The right to rectify their data if inaccurate or processed unfairly.
- Any other information which is necessary so that processing may be fair and to ensure the data subject has all the information that is necessary so as to be aware as to how their data will be processed.

In addition, where the personal data is not obtained from the data subject, either at the time their data is first processed or at the time of disclosure to a third party, all the above information must be provided to the data subject and they must also be informed of the identity of the original data controller from whom the information was obtained, and the categories of data concerned. To fairly process personal data, it must have been fairly obtained, and:

. The data subject must have given consent to the
processing; or

. The processing must be necessary for one of the following reasons: -

- The performance of a contract to which the data subject is a party.
- In order to take steps at the request of the data subject prior to entering into a contract.
- Compliance with a legal obligation, other than that imposed by contract.
- To prevent injury or other damage to the health of the data subject.
- To prevent serious loss or damage to property of the data subject.
- To protect the vital interests of the data subject where the seeking of the consent of the data subject is likely to result in those interests being damaged.
- For the administration of justice.
- For the performance of a function conferred on a person by or under an enactment.
- For the performance of a function of the government or a minister of the government.
- For the performance of any other function of a public nature performed in the public interest by a person.
- For the purpose of the legitimate interests pursued by a data controller except where the processing is unwarranted in any particular case by reason of prejudice to the fundamental rights and freedoms or legitimate interests of the data subject.

To **fairly process sensitive data** (see definitions) it must have been fairly obtained and there are additional special conditions (one of the conditions outlined above must also be met) of which at least one of the following must be met:

The data subject has given explicit consent (or where they are unable to do so, for reasons of incapacity of age, explicit consent must be given by a parent or legal guardian) to the processing, i.e. the data subject has been informed of the purpose/s in processing the data and has supplied his/her data with that understanding; or

the processing must be necessary for one of the following reasons: -

- For the purpose of exercising or performing any right or obligation which is conferred or imposed by law on the data controller in connection with employment.
- To prevent injury or other damage to the health of the data subject or another person, or serious loss in respect of, or damage to, property or otherwise to protect the vital

interests of the data subject or of another person in a case where, consent cannot be given, or the data controller cannot reasonably be expected to obtain such consent.
- To prevent injury to, or damage to the health of, another person, or serious loss in respect of, or damage to, the property of another person, in a case where such consent has been unreasonably withheld.
- It is carried out by a not-for-profit organisation in respect of its members or other persons in regular contact with the organisation.
- The information being processed has been made public as a result of steps deliberately taken by the data subject.
- For the purpose of obtaining legal advice, or in connection with legal proceedings, or is necessary for the purposes of establishing, exercising or defending legal rights;
- For medical purposes (more extensive advice as to what constitutes medical purposes is available from www.dataprotection.ie or you can contact the office directly);
- It is carried out by political parties or candidates for election in the context of an election.
- For the purpose of the assessment or payment of a tax liability.
- In relation to the administration of a social welfare scheme.

2. Keep it only for one or more specified, explicit and lawful purposes

You may only keep data for a purpose(s) that are specific, lawful and clearly stated and the data should only be processed in a manner compatible with that purpose(s). An individual has a right to question the purpose for which you hold his/her data and you must be able to identify that purpose. To comply with this rule:

. In general, a person should know the reason/s why you are collecting and retaining their data.
- The purpose for which the data is being collected should be a lawful one.
- You should be aware of the different sets of data which you keep and specific purpose of each.

3. Use and disclose it only in ways compatible with these purposes

Any use or disclosure must be necessary for the purpose(s) or compatible with the purpose(s) for which you collect and keep the data. You should ask yourself whether the data subject would be surprised to learn that a particular use of or disclosure of their data is taking place. A key test of compatibility is:
- Do you use the data only in ways consistent with the purpose(s) for which they are kept?
- Do you disclose the data only in ways consistent with that purpose(s)?

The rule, that disclosures of information must always be compatible with the purpose(s) for which that information is kept, is lifted in certain restricted cases by Section 8 of the Act. Examples of such cases would include some obvious situations where disclosure of the information is required by law or is made to the individual himself/herself or with his/her consent.

Any processing of personal data by a data processor on your behalf must also be undertaken in compliance with the Acts. This requires that, as a minimum, any such processing takes place subject to a contract between the controller and the processor which specifies the conditions under which the data may be processed, the security conditions attaching to the processing of the data and that the data be deleted or returned upon completion or termination of the contract. The data controller is also required to take reasonable steps to ensure compliance by the data processor with these requirements.

4. Keep it safe and secure

Appropriate security measures must be taken against unauthorised access to, or alteration, disclosure or destruction of, the data and against their accidental loss or destruction. The security of personal information is all-important, but the key word here is appropriate, in that it is more significant in some situations than in others, depending on such matters as confidentiality and sensitivity and the harm that might result from an unauthorised disclosure. High standards of

security are, nevertheless, essential for all personal information. The nature of security used may take into account what is available technologically, the cost of implementation and the sensitivity of the data in question. A minimum standard of security would include the following:

- access to central IT servers to be restricted in a secure location to a limited number of staff with appropriate procedures for the accompaniment of any non-authorised staff or contractors;
- access to any personal data within an organisation to be restricted to authorised staff on a need-to-know basis in accordance with a defined policy;
- access to computer systems should be password protected with other factors of authentication as appropriate to the sensitivity of the information;
- information on computer screens and manual files to be kept hidden from callers to your offices;
- back-up procedure in operation for computer held data, including off-site back-up;
- all reasonable measures to be taken to ensure that staff are made aware of the organisation's security measures, and comply with them;
- all waste papers, printouts, etc. to be disposed of carefully;
- a designated person should be responsible for security and for periodic reviews of the measures and practices in place.

5. Keep it accurate, complete and up-to-date

Apart from ensuring compliance with the Acts, this requirement has an additional importance in that you may be liable to an individual for damages if you fail to observe the duty of care provision in the Act applying to the handling of personal data which tends to arise substantially in relation to decisions or actions based on inaccurate data. In addition, it is also in the interests of your business to ensure accurate data for reasons of efficiency and effective decision making. To comply with this rule, you should ensure that:

- Your clerical and computer procedures are adequate with appropriate cross-checking to ensure high levels of data accuracy.
- The general requirement to keep personal data up-to-date has been fully examined.
- Appropriate procedures are in place, including periodic review and audit, to ensure that each data item is kept up-to-date.

Note:

The accuracy requirement does not apply to back-up data, that is, to data kept only for the specific and limited purpose of replacing other data in the event of their being lost, destroyed or damaged.

6. Ensure that it is adequate, relevant and not excessive

You can fulfil this requirement by making sure you are seeking and retaining only the minimum amount of personal data which you need to achieve your purpose(s). You should decide on specific criteria by which to assess what is adequate, relevant, and not excessive and apply those criteria to each information item and the purpose/s for which it is held.

To comply with this rule, you should ensure that the information sought and held is:

- Adequate in relation to the purpose/s for which you sought it.
- Relevant in relation to the purpose/s for which you sought it.
- Not excessive in relation to the purpose/s for which you sought it.

A periodic review should be carried out of the relevance of the personal data sought from data subjects through the various channels by which information is collected, i.e. forms, website etc. In addition, a review should also be undertaken on the above basis of any personal information already held.

7. Retain it for no longer than is necessary for the purpose or purposes

This requirement places a responsibility on data controllers to be clear about the length of time for which data will be kept and the reason why the information is being retained. It is a key requirement of Data Protection legislation as personal data collected for one purpose cannot be retained once

that initial purpose has ceased. Equally, as long as personal data is retained the full obligations of the Acts attach to it. If you don't hold it anymore then the Acts don't apply.
You should assign specific responsibility to someone for ensuring that files are regularly purged, and that personal information is not retained any longer than necessary. This can include appropriate anonymisation of personal data after a defined period if there is a need to retain non-personal data.
To comply with this rule, you should have:

- A defined policy on retention periods for all items of personal data kept.
- Management, clerical and computer procedures in place to implement such a policy.

8. Give a copy of his/her personal data to that individual, on request

On making an access request any individual about whom you keep personal data is entitled to:

- A copy of the data you are keeping about him or her.
- Know the categories of their data and your purpose/s for processing it.
- Know the identity of those to whom you disclose the data.
- Know the source of the data, unless it is contrary to public interest.
- Know the logic involved in automated decisions.
- Data held in the form of opinions, except where such opinions were given in confidence and even in such cases where the persons fundamental rights suggest that they should access the data in question it should be given.

It is important that you have clear co-ordinated procedures in place to ensure that all relevant manual files and computers are checked for the data in respect of which the access request is being made. To make an access request the data subject must:

- Apply to you in writing (which can include email).
- Give any details which might be needed to help you identify him/her and locate all the Information you may keep about him/her e.g. previous addresses, customer account numbers; Every individual about whom a data controller keeps personal information has a number of other rights under the Act, in addition to the Right of Access. These include the right to have any inaccurate information rectified or erased, to have personal data taken off a direct marketing or direct mailing list and the right to complain to the Data Protection Commissioner.

In response to an access request, you must:

- Supply the information to the individual promptly and within 40 days of receiving the request accompanied by fee of €20.00
- Provide the information in a form which will be clear to the ordinary person, e.g. Any codes must be explained.

If you do not keep any information about the individual making the request you should tell them so within the 40 days. You are not obliged to refund any fee you may have charged for dealing with the access request should you find you do not, in fact, keep any data. However, the fee must be refunded if you do not comply with the request, or if you have to rectify, supplement or erase the personal data concerned.

If you restrict the individual's right of access in accordance with one of the very limited restrictions set down in the Acts, you must notify the data subject in writing within 40 days and you must include a statement of the reasons for refusal. You must also inform the individual of his/her entitlement to complain to the Data Protection Commissioner about the refusal.
There are a number of modifications to the basic Right to Access granted by the Acts which include the following:

- Access to Health and Social Work Data

There are modifications to the right of access in the interest of the data subject or the public interest, designed to protect the individual from hearing anything about himself or herself which might cause serious harm to his or her physical or mental health or emotional well-being;

- In the case of Examinations Data

There is an increased time limit for responding to an access request from 40 days to 60 days and an access request is deemed to be made at the date of the first publication of the results or at the date of the request, whichever is the later.

Appendix 2 - Personal Data Security Breach Report Form

If you discover a personal data security breach, please notify the Data Protection Officer. Please complete this form and return it to the Data Protection Officer as soon as possible.

Notification of Data Security Breach	
Date(s) of Breach:	
Date Incident was discovered:	
Name of Person Reporting Incident:	
Contact Details of Person Reporting Incident:	
Brief Description of Personal Data Security Breach:	
Number of Data Subjects affected – if known:	
Brief Description of any action since breach was discovered:	
Was incident report to the Office of the Data Protection Commissioner?	
For Information Compliance Office Use Only	
Report received by:	
Date:	
Action:	

Date: