Northumberland Golf Club Limited and Gosforth Park Ladies Golf Club
Data Protection and Retention Policy

Context and overview
Key details
The data controllers are the NGC and GPLGC committees
• Policy prepared by: NGC General Manager and GPLGC secretary
• Approved by board / management on: 24th May 2018
• Policy became operational on: 25th May 2018
• Next review date: 1st April 2019

Introduction
NGC and GPLGC need to gather and use certain information about individuals to carry out operation as a golf club. These individuals can include members, customers, suppliers, business contacts, employees and other people the organisation has a relationship with or may need to contact.

These operations include but are not limited to:
Compliance with current legislation
Communication with Government Agencies
Facilitation of payments via the UK Banking System
Performing contracts that the individual and NGC and GPLGC are party to so that NGC and GPLGC can fulfil their legal obligations.
Communicate with the members of NGC and GPLGC.

We regard the above as proper reasons for utilising data NGC and GPLGC have gathered.
This policy describes how this personal data must be collected, handled and stored to meet the company's data protection standards — and to comply with the law.

Why this policy exists
This data protection policy ensures NGC and GPLGC
- comply with data protection law and follow good practice
• protect the rights of staff, customers and partners
• are open about how they store and process individuals' data
• Protect from the risks of a data breach

Data protection law
The EU General Data Protection Regulation describes how organisations — including NGC and GPLGC — must collect, handle and store information.

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

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

The General Data Protection Regulation is underpinned by important principles. These say that data must:

1. Be processed fairly, lawfully and transparently.
2. Be obtained only for specific, explicit and lawful purposes and not processed further in an incompatible manner.
3. Be adequate, relevant and limited to the purpose for which it was collected.
4. Be accurate and, where necessary, kept up to date
5. Kept in a form that permits identification of individuals no longer than necessary.
6. Processed in a manner that ensures technical and organisational security of those data.

Policy scope
This policy applies to:
• The head office of NGC and GPLGC
• All branches of NGC and GPLGC
• All staff and volunteers of NGC and GPLGC
• All contractors, suppliers and other people working on behalf of NGC and GPLGC

It applies to all data that the company holds relating to identifiable individuals, even if that information technically falls outside of the EU General Data Protection Regulation. This can include:
• Names of individuals
• Postal addresses
• Email addresses
• Telephone numbers
- Financial data
- Date of birth
• plus, any other information relating to individuals

Data protection risks
This policy helps to protect NGC and GPLGC from 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 company uses data relating to them.
• Reputational damage. For instance, the company could suffer if hackers successfully gained access to sensitive data.

Responsibilities
Everyone who works for or with NGC and GPLGC has some responsibility for ensuring data is collected, stored and handled appropriately.

Each Data Processor that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

However, these people have key areas of responsibility:
• The board of directors is ultimately responsible for ensuring that NGC and GPLGC meets its legal obligations.

• NGC General Manager and GPLGC committee are responsible for:
o Keeping the board updated about data protection responsibilities, risks and issues.
o Reviewing all data protection procedures and related policies, in line with an agreed schedule.
o Arranging data protection training and advice for the people covered by this policy.
o Handling data protection questions from Data Processors and anyone else covered by this policy.

o Dealing with requests from individuals to see the data NGC and GPLGC holds about them (also called 'subject access requests').
o Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.
o Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
o Performing regular checks and scans to ensure security hardware and software is functioning properly.
o Evaluating any third-party services the company is considering using to store or process data. For instance, cloud computing services.
o Approving any data protection statements attached to communications such as emails and letters.
o Addressing any data protection queries from journalists or media outlets like newspapers.
o Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.

General Data Processor guidelines

- The only people able to access data covered by this policy should be those who need it to carry out their responsibilities.
- Data should not be shared informally. When access to confidential information is required, Data Processors can request it from their Data Controller.
- NGC and GPLGC will provide training to all Data Processors to help them understand their responsibilities when handling data.
- Data Processors should keep all data secure, by taking sensible precautions and following the guidelines below.
- 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 company or externally.
- Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of.
- Data Processors should request help from their Data Controller if they are unsure about any aspect of data protection.
- All Data Processors who have access to data will be given induction training focused on GDPR compliance
- Annual refresher training will take place annually for those deemed necessary.

Data Collection

We may collect personal information about you when you use our services.
This data may include but is not limited to that detailed in Appendix 2.

Data Processing

We will process data that we collect in order to enable the operational procedures of NGC and GPLGC.
NGC and GPLGC have a legitimate interest in processing this data.

Data Sharing

NGC and GPLGC share data that we hold on individuals with other organisations.
These include but are not limited to

England Golf – Governing Body (Central Database of Handicaps)
Accountants – Payroll Processors
Accountants – Auditors
Club Systems -Cloud Based Club Administration Software Provider
BRS – Cloud based Tee booking Software provider.
Members of NGC and GPLGC
Secure Collections – DD Collection agency

Data shared with others is reviewed annually for necessity and access control. Where required access passwords are changed to maintain security.

Data storage

These rules describe how and where data should be safely stored. Questions about storing data safely should be directed to the data controller.

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 a locked drawer or filing cabinet.
• Data Processors should make sure paper and printouts are not left where unauthorised people could see them, like on a printer.
• Data printouts should be shredded and disposed of securely when no longer required.
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 regularly 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.
• Servers containing personal data should be sited in a secure location, away from general office space.
• Data should be backed up frequently. Those backups should be tested regularly, in line with the company's standard backup procedures.
• Data should never be saved directly to laptops or other mobile devices like tablets or smart phones.
• All servers and computers containing data should be protected by approved security software and a firewall.

Data use

Personal data is of no value to NGC and GPLGC unless the business can make use of it.

We may use your personal information to tell you about relevant services provided by NGC and GPLGC.

However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:

• When working with personal data, Data Processors should ensure the screens of their computers are always locked when left unattended.
• Personal data should not be shared informally. In particular, it should never be sent by email, as this form of communication is not secure.
• Data must be encrypted before being transferred electronically. The Data Controller can explain how to send data to authorised external contacts.
• Personal data should never be transferred outside of the European Economic Area.
• Employees should not save copies of personal data to their own computers. Always access and update the central copy of any data.

You can withdraw your consent to NGC and GPLGC to use of your data at any time.

Data accuracy

The law requires NGC and GPLGC to take reasonable steps to ensure data is kept accurate and up to date.

NGC and GPLGC will carry out an annual review of the data that is held to ensure that it is accurate.

The more important it is that the personal data is accurate, the greater the effort NGC and GPLGC should put into ensuring its accuracy.

It is the responsibility of all Data Processors who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

• Data will be held in as few places as necessary. Data Processors should not create any unnecessary additional data sets.
• Data Processors should take every opportunity to ensure data is updated. For instance, by confirming a customer's details when they call.
• NGC and GPLGC will make it easy for data subjects to update the information held about them. For instance, via the company website.
• 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
The law requires NGC and GPLGC to take reasonable steps to ensure data is only retained as long as is necessary.
NGC and GPLGC will carry out an an annual review of the data that is held to ensure that it has not been held longer than necessary.

Record Type	**Retention Period**
Membership Data	5 years post departure
Bank details	5 years post departure
Photographs of Events	Indefinitely
Accident Books	3 years from date of last Entry
Insurance Records	Indefinitely

Payroll	6 years
Minute Books	Indefinitely
Employment Records	6 years from termination
Visitor Books	Indefinitely

Data Breach

When NGC or GPLGC is informed of a data breach then they are obliged to notify the Information Commisioner's Office (ICO) within 72 hours unless the breach is unlikely to result in a risk to the rights and freedom of the data subject. They will also inform the data subject.

Data Destruction

Paper based data that requires destruction is shredded and electronic information deleted and scrubbed from the server.

NGC and GPLGC will carry out an annual review of the data that is held to ensure that it has been disposed of or destroyed when relevant in an acceptable manner.

Subject access requests
All individuals who are the subject of personal data held by NGC and GPLGC are entitled to:
• Ask what information the company holds about them and why.
• Ask how to gain access to it.
• Be informed how to keep it up to date.
• Be informed how the company is meeting its data protection obligations.

If an individual contacts the company requesting this information, this is called a subject access request. Subject access requests from individuals should be made by email, addressed to the data controller at gm@thengc.co.uk. The data controller can supply a standard request form, although individuals do not have to use this. The data controller must provide the relevant data within 30 days. The data controller will always verify the identity of anyone making a subject access request before handing over any information.

Disclosing data for other reasons
In certain circumstances NGC and GPLGC are allowed to disclose personal data to law enforcement agencies without the consent of the data subject.
Under these circumstances, NORTHUMBERLAND GOLF CLUB and GPLGC will disclose requested data. However, the data controller will ensure the request is legitimate, seeking assistance from the board and from the company's legal advisers where necessary.

Providing information
NGC and GPLGC aim 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