NORTH LANARKSHIRE LIMITED
DATA PROTECTION POLICY

Doc Ref	**NLL-DPP**	**Date**	
File Name	**Data Protection Policy**		

Category	**Information IT Security**
Section	**IT**

Author	
Business Owner	**North Lanarkshire Leisure**
Authorised by	Head of Finance and IT
Authorisation Date	

CONTENTS

1. Policy statement

1.1 This policy sets out and formalises North Lanarkshire Leisure's (NLL) approach to managing personal data in accordance with the requirements of the Data Protection Act 1998 and the General Data Protection Regulations (GDPR). The organisation is committed to being transparent about how it collects and uses personal data and to meeting its data protection obligations.

1.2 This document also outlines NLL's commitment to the principles enshrined within the legislation and the need to balance the rights of individuals with the functions and operational requirements of the organisation.

2. Scope

2.1 This policy applies to:

- All personal data held, maintained and used by NLL in all locations and in all media (hardcopy and electronic).
- All NLL staff, including casual workers, temporary staff, contractors, consultants and volunteers who access and use NLL information; and
- All third parties who manage and process personal data on NLL's behalf when carrying out a statutory function or service

3. Definitions

Data Controller – a legal person or organisation who determines the purposes for which, and manner in which, personal information is to be processed. This may be an individual or an organisation. Data Controllers can process personal data jointly with other data controllers for specified purposes. NLL is a data controller.

Data Processor – is a person, other than an employee of NLL, who processes personal data on behalf of the organisation. This processing must be evidenced in a written contract. The data processor can only use personal data under the instructions of NLL. NLL retains full responsibility for the actions of the data processor in relation to the personal data.

Data Protection Act 1998 – gives effect in the UK law to the EC Directive 95/46/EC and came into force on 1 March 2000 repealing the Data Protection Act 1984. The Data Protection Act 1998, together with a number of Statutory Instruments, requires data controllers to comply with the legislation governing how personal data is used for statutory and business purposes. Amendments have also been created by other legislation such as the Freedom of Information Act 2000. It gives rights to individuals in relation to how organisations can use their personal data.

Data Subject – is a living individual who can be identified from the personal data or from additional information held, or obtained, by NLL.

Enforcement Notice – The Information Commissioner has the power to serve an enforcement notice on a data controller if he determines that a data controller has failed

to comply with the requirements of the Data Protection Act 1998. The Notice sets out the actions that a data controller must take to achieve compliance. A data controller can lodge an appeal against the Notice to the Information Tribunal. It is a criminal offence for a data controller to fail to comply with a valid Enforcement Notice.

General Data Protection Regulation (GDPR) – is the new data protection regulation which will come into force in May 2018. It builds upon, and strengthens, the compliance regime provided by the Data Protection Act 1998.

Information Commissioner - is the independent regulator responsible for ensuring all organisations comply with the Data Protection Act. Organisations are required to notify the ICO of how they process personal data and if they breach the Act. The Commissioner has been granted enforcement powers regarding non-compliance, these include the ability to issue information and enforcement notices, impose large fines (up to £500,000), and bring a criminal case against an organisation. Further information about data protection is available on the ICO website at www.ico.org.uk.

Information Notice – an Information Notice can be issued by the Information Commissioner which requires a data controller to provide his office with information that he requires to carry out his functions. Failure to comply with an Information Notice is a criminal offence.

Information Security – ensures that NLL information is not compromised by unauthorised access, modification, disclosure or loss.

Information (or data) Sharing – ensures that NLL information is shared in a compliant, controlled and transparent manner.

Notification – is the process by which organisations notify the Information Commissioner about the categories of personal information it processes and the purposes the personal information is being processed for. The Information Commissioner uses this information to maintain a Register of Data Controllers which it publishes on its website.

Personal data (or information) – is information about a living individual who can be identified from that information or from additional information held, or obtained, by NLL. Examples of personal data are contained in paper files, electronic records and visual and audio recordings.

Privacy Impact Assessment – is a risk management tool that reduces the risks of harm to individuals through the misuse of their personal information. It assists in designing appropriate processes for handling personal data. It is used when projects, or changes to service activities, or new ICT impact on the privacy of individuals

Processing – is all actions relating to personal data. Gathering, recording, analysing, amending, using, sharing, disclosing, storing and destroying personal data are all covered by this definition.

Special Category (Sensitive) personal data – requires a higher level of consideration. Information will be considered 'sensitive personal data' if it relates to a person's: racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition, sexual life, and criminal offences or alleged criminal activity (including any criminal proceedings).

Subject Access Request (SAR) - the right granted to an individual by the Data Protection Act 1998 to request a copy of personal information held about them.

4. Data Protection Principles

4.1 Under the GDPR, the data protection principles set out the main responsibilities for organisations.

4.2 Article 5 of the GDPR requires that personal data shall be:

a) processed lawfully, fairly and in a transparent manner in relation to individuals;

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

f) 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.

4.3 Article 5(2) requires that:

"the controller shall be responsible for, and be able to demonstrate, compliance with the principles."

4.4 NLL regularly collects and processes personal data from individuals who receive services or have a relationship with the organisation (e.g. suppliers, employees). However, NLL will only obtain, use and retain personal information that it actually needs

to fulfil its business and operational requirements.

4.5 A Privacy Impact Assessment (PIA) will be completed when processes or services that involve personal data are designed or revised. The PIA will identify and document appropriate governance controls required to manage the privacy risks associated with the process.

4.6 Specifically, a PIA must be carried out by service areas when:

- NLL projects or programmes are undertaken
- Service activities commence, end or are significantly adjusted; and/or
- New ICT arrangements are put in place which use and process personal data with a potential impact on the privacy of individuals

5. Informing data subjects & Fair processing

5.1 When collecting personal data, the organisation will inform data subjects about why their personal data is required and how it will be used and retained. It will also explain whether the personal data will be shared. This is called a Fair Processing Notice or Privacy Statement.

5.2 Appropriate fair processing information will be provided at the time personal data is collected from data subjects, or when NLL first contacts the data subject in relation to the personal data they have provided.

5.3 It is recognised that in order to provide customers with a better service, personal data collected across the organisation may be used in different ways, if its use is deemed appropriate and fair.

5.4 In such cases, data subjects will be advised if their personal data is to be used in a new way.

5.5 Fair processing information must be approved by the Head of Finance and IT and documented within the relevant PIA.

6. Sharing Personal Data with other organisations

6.1 NLL works with other organisations to provide services. The sharing of personal data with third parties is subject to formal information sharing protocols. These set out overarching common rules adopted by NLL and its partners with whom it wishes to share data.

6.2 Details of each data sharing process are documented in information sharing agreements. A central register of all protocols and agreements will be maintained by the Head of Finance and IT to ensure that transfer and sharing arrangements meet the requirements of the Data Protection Act 1998, and the Information Commissioner's Code of Practice on Data Sharing.

6.3 All new data sharing protocols and agreements must be assured by the Head of Finance and IT before they are signed/ used.

7. Disclosing Personal Data

7.1 There are many instances where it will be fair and reasonable to disclose personal data with (and without) the consent of the individual. All requests for personal data and disclosures must be documented.

7.2 Information may be shared through partnership arrangements where there is a data sharing agreement in place or where the individual has authorised disclosure through a mandate.

7.3 When disclosing personal data, NLL will only disclose personal data that is necessary for the stated purpose.

7.4 Data subjects can request access to their own personal data; this is known as a Subject Access Request (SAR). For information about SARs, and other rights of access to information.

8. Disclosure of personal data relating to crime, or required by law

8.1 Section 29 of the Act allows NLL to consider disclosing personal data for the purpose of prevention and detection of crime; the apprehension or prosecution of offenders; or the assessment or collection of taxes or duties.

8.2 Section 35 of the Act allows the organisation to disclose personal data if it is required for legal proceedings.

8.3 Each request is considered on a case by case basis and must be forwarded to the PA/FOI Officer for processing and response.

9. Individual rights

9.1 As a data subject, individuals have a number of rights in relation to their personal data.

Subject access requests

9.2 Individuals have the right to make a subject access request. If an individual makes a subject access request, the organisation will tell him/her:

- whether or not his/her data is processed and if so why, the categories of personal data concerned and the source of the data if it is not collected from the individual;
- to whom his/her data is or may be disclosed, including to recipients located outside the European Economic Area (EEA) and the safeguards that apply to such transfers;
- for how long his/her personal data is stored (or how that period is decided);
- his/her rights to rectification or erasure of data, or to restrict or object to processing;
- his/her right to complain to the Information Commissioner if he/she thinks the organisation has failed to comply with his/her data protection rights; and
- whether or not the organisation carries out automated decision-making and the logic involved in any such decision-making.

9.3 The organisation will also provide the individual with a copy of the personal data

undergoing processing. This will normally be in electronic form if the individual has made a request electronically, unless he/she agrees otherwise. [If the individual wants additional copies, the organisation will charge a fee, which will be based on the administrative cost to the organisation of providing the additional copies.]

9.4 To make a subject access request, the individual should send the request to info@nlleisure.com. In some cases, the organisation may need to ask for proof of identification before the request can be processed. The organisation will inform the individual if it needs to verify his/her identity and the documents it requires.

9.5 The organisation will normally respond to a request within a period of one month from the date it is received. In some cases, such as where the organisation processes large amounts of the individual's data, it may respond within three months of the date the request is received. The organisation will write to the individual within one month of receiving the original request to tell him/her if this is the case.

9.6 If a subject access request is manifestly unfounded or excessive, the organisation is not obliged to comply with it. Alternatively, the organisation can agree to respond but will charge a fee, which will be based on the administrative cost of responding to the request. A subject access request is likely to be manifestly unfounded or excessive where it repeats a request to which the organisation has already responded. If an individual submits a request that is unfounded or excessive, the organisation will notify him/her that this is the case and whether or not it will respond to it.

Other rights

9.7 Individuals have a number of other rights in relation to their personal data:

- the right to be informed;
- the right of access;
- the right to rectification;
- the right to erasure;
- the right to restrict processing;
- the right to data portability;
- the right to object ; and
- the right not to be subject to automated decision-making including profiling.

9.8 To ask the organisation to take any of these steps, the individual should send the request to info@nlleisure.com.

10. Unauthorised Disclosure

10.1 Employees (and others covered by this policy) must never disclose personal data obtained in the course of their work with NLL, or access personal data without appropriate permissions. It is a criminal offence to knowingly obtain or disclose personal data without the consent of the data controller (NLL).

11. Security

11.1 NLL will ensure that appropriate controls are in place to keep personal data secure at all times.

11.2 NLL's policies on Information Security, including ICT Acceptable Use, must be followed at all times. Particular care should be given to the display and transportation of personal

data to ensure that unauthorised access or disclosure is not made whether by accident or design.

12. Reporting and Managing Data Protection Breaches

12.1 A Data Protection Breach can occur through the theft or accidental loss of personal data (for example, laptops, tablets, portable devices, files containing personal data). They can also occur through the unauthorised use or accidental disclosure of personal data by employees, or deliberate attacks on NLL systems.

12.2 All Data Protection Breaches must be reported to the Head of Finance and IT immediately. This will allow the organisation to take all the necessary steps to recover the data and limit any potential damage caused by the breach.

13. Data Processors

13.1 Contractors and consultants will carry out work and process personal data on NLL's behalf to help deliver services. In such cases, NLL is considered to be the 'data controller' responsible for that personal data, and the contractor or consultant is the 'data processor' who processes the data on behalf of NLL.

13.2 Such arrangements must be governed by written agreements or contracts to ensure compliance with this policy and the data protection principles, including on-going monitoring.

14. Records Management

14.1 All personal data must be held, retained and reviewed in accordance with the NLL's Records Management Policy and agreed retention schedules.

15. Information Asset Register

15.1 An Information Asset Register will be maintained by the Head of Finance and IT. The register identifies personal data and sensitive personal data held by NLL, and helps to evaluate and assure compliance with the organisation's information governance policies and processes, recording and highlighting risk as appropriate.

16. Roles and responsibilities

16.1 This section provides a summary of specific responsibilities in relation to compliance with the Data Protection Act 1998, GDPR and this policy.

Head of Finance and IT

16.2 The Head of Finance and IT has responsibility for the day to day operation and delivery of information governance within NLL. In relation to data protection it will:

- Act as the first point of contact for all data protection issues affecting the organisation;

- Provide guidance and advice on data protection issues for the organisation;
- Renew and amend the organisation's data protection notification to the ICO, as advised by managers;
- Co-ordinate, process and respond to all subject access requests;
- Oversee and quality assure all data sharing protocols and agreements between the organisation and other partner agencies;
- Record and maintain the organisation's information risk register, including risks relating to data protection and associated information governance activities;
- Create, maintain and renew training modules and toolkits as appropriate;
- Provide data protection training and raise awareness through regular communications
- Maintain and report on key performance indicators for information governance;
- Lead and advise on compliance requirements where the processing of personal data is complex (e.g. multi-agency working);
- Co-ordinate the organisation's information breach procedures;
- Carry out information governance assessments;
- Record and maintain the organisation's register of information sharing agreements; and
- Record and maintain the organisation's register of Privacy Impact Assessments.

Managers

16.3 All managers must:

- Ensure that this policy and any associated procedures governing the use of personal information (corporate and local) are in place, understood and followed by all staff within their business areas.
- Ensure that their staff have received data protection training (appropriate to their role), and maintain records as to when initial and refresher training has taken place;
- Review and revise procedures if processes governing the use of personal information are subject to change within their business areas;
- Consult the Head of Finance and IT when there is a proposed change to the use of personal information, or when new projects are being considered;
- Undertake Privacy Impact Assessments in respect of new projects or new processing of personal information;
- Consult the Head of Finance and IT before signing up to, or revising, and information sharing protocol or agreement;
- Report any suspected breaches of confidentiality or information loss to the Head of Finance and IT and follow the breach reporting procedure;

- Identify any existing or emerging information risks relating to personal information and report to the Head of Finance and IT and, if required, record on risk registers;
- Ensure that personal data required to answer a subject access request is provided timeously to the Head of Finance and IT;
- Ensure that there are appropriate procedures and measures in place to protect personal data, particularly when that information (hardcopy and electronic) is removed from NLL premises;
- Undertake annual information governance self-assessments to ensure ongoing compliance with this policy and associate information governance activities;
- Provide a statement of assurance to evidence information governance compliance; and
- Inform the Head of Finance and IT (when requested) of activities containing personal data (paper or electronic) to facilitate NLL's notification process with the Information Commissioner.

Staff

16.4 All staff have responsibility for data protection and must:

- Read, understand and follow this policy and any associated procedures that relate to the use and handling of personal information in the course of their work;
- Undertake data protection training (including annual refresher training) and ensure they have a clear understanding of their responsibilities in using and handling personal information;
- Identify and report any risks to personal information to their line manager Identify and report suspected breaches of confidentiality or compromised personal data to their line manager;
- Identify and forward any subject access requests to the PA/FOI Officer to ensure that requests can be processed in accordance with statutory timescales; and
- Assist customers in understanding their information rights and the organisation's responsibilities in relation to data protection.

17. Risk assessment

17.1 Failure to comply with any requirement of the Act/Regulations could result in enforcement action by the ICO. The ICO has powers to impose a Civil Monetary Penalty which can result in a fine. There will be two levels of fines based on the GDPR. The first is up to €10 million or 2% of the company's global annual turnover of the previous financial year, whichever is higher. The second is up to €20 million or 4% of the company's global annual turnover of the previous financial year, whichever is higher.

17.2 Individuals may take action against NLL through the Court for any misuse of their personal data. Depending on which Court takes the action, fines could be unlimited.

17.3 Failure to respond to any of the time critical response requirements in relation to information rights for individuals will result in a breach of the Act.

17.4 Mishandling of personal information will have serious reputational impact to the organisation.

17.5 Mishandling of personal information may have serious implication to one, or more, individuals.

17.6 Personal information that is inaccurate or out of date may result in a serious negative impact on one or more individuals.

18. Training

18.1 All employees, contractors, consultants and volunteers need to be aware of their obligations under the Act/Regulations. A variety of training methods will be employed to ensure appropriate levels of awareness, understanding and knowledge.

19. Review

19.1 This policy will be reviewed annually or more quickly if required by significant changes in legislation, regulation or business practice. It will be reviewed by the Head of Finance and IT and presented to the Board of Directors.