DATA PROTECTION POLICY - DELIVERED ON A BEST ENDEAVOURS BASIS

1. Objective of this Policy

The purpose of this policy is to outline how Middlesex County RFU Limited ('the County') has established measures to maintain compliance with The Data Protection Act 2018 and the EU General Data Protection Regulation ('GDPR').

The policy contains three components:

- Section A – Measures to re-enforce accountability and governance measures
- Section B – Measures to demonstrate the protection of information rights of the data subject
- Appendix A & B – Day to day guidance for Volunteers.

2. Scope

The Policy relates to all Officers, Management Board members, Committee Members, County Employees and Volunteers carrying out activities for the County.

3. Audience for this Policy

All Officers, Management Board members, Committee Members and County Employees. People carrying out activities for the County ('Volunteers') are also included.

4. Principles

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

- Processed lawfully, fairly and in a transparent manner in relation to individuals
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
- 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, amended, erased or rectified without delay

- 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, in line our Data Retention Policy. 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
- 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.

In addition, there is a requirement that:

- 'The controller shall be responsible for, and be able to demonstrate, compliance with the principles.'

5. SECTION A - ACCOUNTABILITY AND GOVERNANCE

This policy outlines comprehensive but proportionate governance measures designed to achieve and maintain compliance with the GDPR. These measures have been designed to minimise the risk of breaches and uphold the protection of personal data.

This section on accountability and governance considers:

- Roles and responsibilities – the responsibilities of the Middlesex Management Board, Data Protection Officer, information owners, Volunteers and employees
- Documentation – the County's requirements in respect of documenting processing
- Data protection by design and default - the County's requirements for Data Protection Impact Assessments
- Lawful basis for processing – the County's policy on determining the basis for processing
- Security – measures designed to protect information confidentiality, integrity, and availability
- Contracts – the measures that should be in place to ensure contractual relationships maintain GDPR compliance
- International transfer – oversight measures for international transfer of data
- Data breaches – principles for detecting and responding to data breaches.

5.1 Roles and responsibilities

Background

While the principles of accountability and transparency have previously been implicit requirements of data protection law, the GDPR's emphasis elevates their significance. The County is expected to put into place comprehensive but proportionate governance measures.

Policy requirements

- The County has assessed the need to appoint a Data Protection Officer and concluded that it does not need to do so because the County:
    - Is not a public authority
    - Does not as, a core activity, carry out large scale, regular and systematic monitoring of individuals
    - Does not, as core activity, carry out large scale processing of special categories of data or data relating to criminal convictions and offences.
- The County Secretary has been made responsible for certain data protection activities of the County. The County Secretary's responsibilities include:
    - Advising the 'Volunteers' (refer to Appendix A) about their obligations to comply with the GDPR and other data protection laws
    - Monitoring compliance with the GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits
    - Acting as the first point of contact for supervisory authorities and for individuals whose data is processed.
- The County Secretary reports to the Middlesex Management Board on a regular basis on data protection matters.

5.2 Documentation

Background

The GDPR contains explicit provisions about documenting the County's processing activities. The County must maintain records on several things such as processing purposes, data sharing and retention. The County may be required to make the records available to the ICO on request.

Policy requirements

- Where the County is a controller for personal data, the County maintains documentation in a manner consistent with Article 30(1) of the GDPR
- Where the County is processor for personal data, the County maintains documentation in a manner consistent with Article 30(2) of the GDPR
- If the County processes special category or criminal conviction and offence data, the County documents:
    - The condition for processing under the Data Protection Act 2018
    - The lawful basis for processing
    - Whether the personal data is erased and retained in accordance with the County policy

- The County conducts regular reviews of the personal data processed and updates documentation accordingly.

5.3 Data protection by design and default

Background

Under the GDPR, the County has a general obligation to implement technical and organisational measures to show that the County has considered and integrated data protection into processing activities.

Policy requirements

- The County carries out a Data Protection Impact Assessment ('DPIA') when:
    - Using new technologies and the processing is likely to result in a high risk to the rights and freedoms of individuals
- Processing that is likely to result in a high risk includes (but is not limited to):
    - Systematic and extensive processing activities, including profiling and where decisions that have legal effects, or similarly significant effects on individuals
    - Large scale processing of special categories of data or personal data relation to criminal convictions or offences. This includes processing a considerable amount of personal data at regional, national, or supranational level that affects a large number of individuals and involves a high risk to rights and freedoms (e.g., based on the sensitivity of the processing activity)
    - Large scale, systematic monitoring of public areas (CCTV)
- The decision of whether to conduct a DPIA is supported by a documented risk assessment and is endorsed by the County Secretary.

5.4 Lawful basis for processing

Background

Under the GDPR, there are six available lawful bases for processing. The County has documented the relevant lawful basis for processing and the purpose of that processing in its Information Asset Register.

The lawful bases for processing are set out in Article 6 of the GDPR. At least one of these must apply whenever the County processes personal data:

a) **Consent –** the individual has given clear consent for you to process their personal data for a specific purpose

b) **Contract –** the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract

c) Legal obligation – the processing is necessary for you to comply with the law (not including contractual obligations)

d) Vital interests – the processing is necessary to protect someone's life

e) **Public task –** the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law

f) Legitimate interests – the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

Policy requirements

- The County privacy notice includes the lawful basis for processing as well as the purposes of the processing
- The County only processes personal information to enable it, as an organisation, to administer its business, maintain its accounts and records and support and manage its Volunteers and employees
- The County only processes information relevant to the above purposes. This may include:
    - Personal details
    - Education and employment details
    - Business activities of the person whose personal data is being processed
    - Financial details
    - Goods or services provided
- The County may also process sensitive classes of information that may include details of physical or mental health
- The County only processes personal information about its:
    - Volunteers and employees
    - Professional advisers
    - Suppliers and service providers
    - Players, or those engaging in rugby activity.
- The personal information processed may be shared with the individuals themselves and also with other organisations. Where this is necessary the County comply with all aspects of the Data Protection Act (DPA)
- Where necessary or required the County shares information with:
    - Family, associates and representatives of the person whose personal data is being processed
    - Current, past and prospective employers
    - Ombudsman and regulatory authorities
    - Suppliers and service providers.

5.5 Security

Background

The GDPR requires personal data to be processed in a manner that ensures its security. This includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage. It requires that appropriate technical or organisational measures are used.

Policy requirements

- The County requires its outsourced service suppliers to have defined and implemented an information security policy and supporting management system to maintain effective and proportionate security.

5.6 Contracts

Background

The GDPR requires diligence and clarity in entering into third party relationships. Whether the County is a processor or controller, there are mandatory requirements relating to the contracts that are in place.

Policy requirements

- Whenever the County acts as a controller a written contract must be in place with the processors. The standards to be applied to the contracts have been defined by the Information Commissioner's Office
- Whenever the County acts as a processor, the County must only act on the documented instructions of a controller (as specified in a valid written contract). Standards to be applied to the contracts have been defined and are documented by the Information Commissioner's Office.

5.7 Data breaches

Background

A personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This means that a breach is more than just losing personal data.

The GDPR will introduce a duty on all organisations to report certain types of data breach to the relevant supervisory authority. In some cases, organisations will also have to report certain types of data breach to the individuals affected.

Policy requirements

- The County Secretary must be notified of all breaches to this policy as soon as possible
- The County Secretary must record breaches and work with the information owner to consider the likely impact of the breach
- Where a breach is considered notifiable to the Information Commissioner, the County Secretary must immediately inform the Board
- Where the County acts a 'Data Controller', a notifiable breach has to be reported by the County

Secretary to the relevant supervisory authority within 72 hours of the County becoming aware of it. The notification must contain:

  - The nature of the personal data breach including, where possible the following:
    - The categories and approximate number of individuals concerned
    - The categories and approximate number of personal data records concerned
  - The name and contact details of the data protection or other contact point for more information
  - A description of the likely consequences of the personal data breach
  - A description of the measures taken, or proposed to be taken, to deal with the personal data breach and, where appropriate, of the measures taken to mitigate any possible adverse effects

- Where a breach is likely to result in a high risk to the rights and freedoms of individuals, the County will notify those concerned directly
- The County Secretary must present an analysis of breaches and near misses to the board at least annually
- All employees must be trained to recognise and escalate breaches.

5.8 Compliance and reporting

Background

Monitoring compliance with the GDPR is a key role of the County Secretary and must also report compliance to the Board.

Policy requirements

- The County Secretary is responsible for developing a compliance monitoring plan for this policy
- The compliance monitoring plan should be submitted to the Board for approval
- Progress to deliver the plan, exceptions noted, breaches and near misses and updates on progress to address material deviations from compliance with the policy must be reported to the County Secretary to the Board.

5.9 Training and awareness

Background

Employee awareness of the GDPR, and their role to protect the privacy of data subjects, is core to the County's compliance programme.

Policy requirements

- Employees must be trained on the requirements of this policy regularly.

6. SECTION B – INDIVIDUAL RIGHTS

The GDPR provides the following rights for individuals:

- The right to be informed
- The right of access
- The right to rectification
- The right to erase
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling.

6.1 Right to be informed

Background

The right to be informed encompasses the County's obligation to provide 'fair processing information', typically through a privacy notice.

Policy requirements

- The County maintains a privacy notice and publishes this publicly and on request.

6.2 Right of access

Background

Individuals have the right to access their personal data and supplementary information. The right of access allows individuals to be aware of and verify the lawfulness of the processing.

Under the GDPR, individuals will have the right to obtain:

- Confirmation that their data is being processed
- Access to their personal data
- Other supplementary information – this largely corresponds to the information that should be provided in a privacy notice.

Policy requirements

- All requests from subjects for access to their data ('Subject Access Request' (SAR)) should be submitted immediately to the County Secretary. The County Secretary must log the request and will:
    - Consider whether the request is manifestly unfounded or excessive
    - Request copies of information held from information owners within the County

- Review the information to ensure it does not impair the privacy of another data subject
- Consider whether the request warrants a fee (if it requires a significant amount of data)
- Respond to the original request.

- A response to the request must be provided without delay and at the latest within one month of receipt. In the event the request is particularly complex or numerous, the period of compliance can be extended by a further two months. If this is the case, the County Secretary must inform the individual within one month of the receipt of the request and explain why the extension is necessary
- Performance against the response target of one month must be reported to the Board by the County Secretary at least annually.

6.3 Right to rectification

Background

The GDPR gives individuals the right to have personal data rectified if it is inaccurate or incomplete.

Policy requirements

- Requests for rectification must be treated in the same way as requests for access. The following additional measures will apply:
  - If the County has disclosed the personal data in question to third parties, the County Secretary must inform them of the rectification where possible
  - The County Secretary must also inform the individuals about the third parties to whom the data has been disclosed where appropriate
  - The information owner will be responsible for ensuring the request for rectification are actioned on the information they are responsible for
  - The County Secretary will be responsible for validating whether requests for rectification have been properly addressed.

6.4 Right to erasure

Background

The right to erasure is also known as 'the right to be forgotten'. The broad principle underpinning this right is to enable an individual to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

The right to erasure does not provide an absolute 'right to be forgotten'. Individuals have a right to have personal data erased and to prevent processing in specific circumstances. These include:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed
- When the individual withdraws consent

- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing
- The personal data was unlawfully processed (i.e., otherwise in breach of the GDPR)
- The personal data has to be erased in order to comply with a legal obligation
- The personal data is processed in relation to the offer of information society services to a child.

Policy requirements

- The County can refuse to comply with a request for erasure where the personal data is processed for the following reasons:
    - To exercise the right of freedom of expression and information
    - To comply with a legal obligation for the performance of a public interest task or exercise of official authority
    - For public health purposes in the public interest
    - Archiving purposes in the public interest, scientific research historical research or statistical purposes
    - The establishment, exercise or defence of legal claims
- Requests for erasure of data should be submitted immediately to the County Secretary and will follow the same principles as for right to access and right to rectification
- If the County has disclosed the personal data in question to third parties, the County Secretary must inform them about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so.

6.5 Right to restrict processing

Background

Individuals have a right to 'block' or suppress processing of personal data. When processing is restricted, the County is permitted to store the personal data, but not further process it.

The County is required to restrict the processing of personal data in the following circumstances:

- Where an individual contest the accuracy of the personal data, the County should restrict the processing until the County has verified the accuracy of the personal data
- Where an individual has objected to the processing (where it was necessary for the performance of a public interest task or purpose of legitimate interests), and the County considers whether its legitimate grounds override those of the individual
- When processing is unlawful, and the individual opposes erasure and requests restriction instead
- If the County no longer needs the personal data but the individual requires the data to establish, exercise or defend a legal claim.

Policy requirements

- Requests to restrict processing will be submitted to the County Secretary and will follow the same principles as for right to access and right to rectification, with the following additional requirements:
    - The County Secretary must inform individuals when the County decides to lift a restriction on processing.

6.6 Right to data portability

Background

The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.

The right to data portability applies:

- To personal data an individual has provided to a controller
- Where the processing is based on the individual's consent or for the performance of a contract
- When processing is carried out by automated means.

Policy requirements

- Requests for data under the right to data portability must be submitted to the County Secretary
- The County Secretary is responsible for recording these and requesting the information from the information owner(s)
- The County Secretary will also review the data to ensure the privacy of other data subjects is not adversely impacted
- The County Secretary will provide the personal data in a structured, commonly used and machine-readable form, submitted using a secure transfer mechanism
- The information will be provided within one month of the original request
- Performance against this timescale must be reported by the County Secretary to the Board at least annually.

6.7 Right to object

Background

Individuals have the right to object to:

- processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling)
- direct marketing (including profiling)
- processing for purposes of scientific/historical research and statistics.

Policy requirements

- Requests that object to processing must be submitted to the County Secretary
- The County Secretary is responsible for recording and assessing these
- Where instructed by the County Secretary, the County will stop processing the personal data unless:
    - There are demonstrable and compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual
    - The processing is for the establishment, exercise or defence of legal claims
- The County must inform individuals of their right to object 'at the point of first communication' and in its privacy notice.

6.8 Rights relating to automated decision-making including profiling

Background

The GDPR has provisions on:

- Automated individual decision-making (making a decision solely by automated means without any human involvement)
- Profiling (automated processing of personal data to evaluate certain things about an individual) - profiling can be part of an automated decision-making process.

The GDPR has additional rules to protect individuals if an organisation is carrying out solely automated decision-making that has legal or similarly significant effects on them. The County can only carry out this type of decision-making where the decision is:

- Necessary for the entry into or performance of a contract
- Authorised by Union or Member state law applicable to the controller
- Based on the individual's explicit consent.

The County must make sure that it:

- Gives individuals information about the processing
- Introduces simple ways for them to request human intervention or challenge a decision
- Carries out regular checks to make sure that the County systems are working as intended.

Policy requirements

- The County currently carries out no profiling or automated decision-making activity.

6.9 Complaints

Any complaints should be forwarded to the County Secretary at Middlesex County.

6.10 Owner of this Policy

The County Secretary owns this Policy and will review and update it as required on an annual basis for approval by the Middlesex Management Board.

6.11 Document Approval History

Date	Version	Document Approver	Comment
11 April 21	Version 1.3	Middlesex Management Board	To be reviewed in 12 months or updated upon request.

7. APPENDIX – DAY TO DAY GUIDANCE FOR 'VOLUNTEERS'

In the role of 'Volunteer' (as defined above) they are likely to be in possession of contact lists and data that identifies various individuals. This constitutes personal data under GDPR and should be treated confidentially and securely.

Volunteers need to be aware of their obligations under the law and these guidelines. This guidance is based on best practice but may not necessarily be exhaustive. Please use your common sense when handling individual's data either on your PC, laptop, mobile device or paper. Keep it secure and confidential.

7.1 Do not share individual's private data without their consent

Some common-sense guidance is provided below:

- If sharing data, consent needs to be explicit, recorded and retained
- Try to send messages individually, taking care to ensure that email addresses are not inadvertently shared without prior agreement
- If sending group emails, use blind copy so individual's email addresses are not shared
- Volunteers are not required to purge email addresses which are stored in Outlook or the chosen email platform each and every time they have satisfied their purpose, although all are asked to manage their contact data appropriately
- If you set up private social media groups (Facebook, Twitter, WhatsApp, etc.) for conducting communications or sharing information (e.g. to organise training sessions or match day itineraries) make sure that individuals know their data will be known by others in the group when they opt in. They must also be able to opt out
- Social media groups should only include members who have relevance within the group. Group memberships should be monitored regularly
- Social media groups should only exist for as long as they are relevant (and have a necessary legitimate use)
- If individuals post to public Middlesex social media groups, the position is that they have chosen to share their personal data on that platform. If Volunteers use this data to make contact outside of the platform, they should treat it as private.

7.2 For Volunteers and Players under 18 all contact information should be registered with the County Office

All information regarding under 18-year-old players or Volunteers associated with the Middlesex Rugby Community should be registered at the County Office who will retain the master records and associated consent:

- Youth's over the age of 12 are deemed under the legislation to be able to give their own consent. Unless the youth has given consent their parent/guardian is not allowed to see their private information held by the County
- U18 players contact details should not be shared with individuals in the same group unless they explicitly give consent. This consent should be sent to the County Office for registration and safe keeping
- If organising travel or meeting arrangements for a youth their details should not be shared with other individuals within the group or their parents unless explicit consent is given. Consent should be in writing or email and forwarded to the County Office.

7.3 Keeping individual's private data secure

Volunteers have an obligation to keep private data secure:

- If Volunteers have private data on their own device, they should keep it securely. This means keeping the data on a password protected device or in a locked draw/ cabinet. Devices and papers containing private data should not be left unlocked and unattended
- Passwords should be robust and never shared with others who could gain access to the private data. If a password is compromised it should be changed at the earliest opportunity.

7.4 Loss of private data, data breaches and data access requests

- If a Volunteer receives a request from an individual to see the data that the County holds on them, the request should be passed to the County Office as soon as possible. The County Office will discuss with the County Secretary how best to fulfil the data access request. The Volunteers should not attempt to fulfil the request themselves but simply advise the individual that the request has been passed to the County Office
- If a Volunteer receives a request from an individual to have their data amended or deleted, this request should be passed to the County Office who will manage the changes to the data
- Should there be a loss/theft of data (i.e., loss of a mobile device or hacking of a PC containing private data) or an individual's data be inappropriately shared with others (i.e., email address shared by accident), this must be reported to the County Office immediately where the County Secretary will determine if a data breach has occurred and if this needs to be reported to the Information Commissioner's Office.

8. Appendix B - Practical tips for data protection

- Obtain and process the information fairly and honestly
- Keep it only for specified and lawful purposes
- Process it only in ways compatible with the purposes for which it was given to you
- Keep it safe and secure
- Keep it accurate and up to date
- Ensure that it is adequate, relevant and not excessive
- Retain it no longer than is necessary for the specified purpose
- Give a copy of his/her personal data to any individual on request.