Data Protection Policy

Final

Scope	Everton FC	Everton Women	EitC	EFS
Staff Group	✓	✓	✓	✓

References in this Policy to "the Club" shall be construed as referring to the relevant entity within the Everton Family for which the employee in question works.

Version Control

Version	Date	Author	Status	Changes from previous version
1.0	February 2018	Ian Garratt	Withdrawn	First Version
1.1 – 1.4	February 2018	Ian Garratt	Withdrawn	Minor amendments
2.0	March 2021	Ian Garratt	Ratified	Updates for Brexit, COVID and minor amendments

February 2018

PRIVATE & CONFIDENTIAL

1 Purpose

Everton Football Club, Everton in the Community, Everton Ladies and Everton Free School (**the Everton Family**) is **committed to protecting the personal data of all of its stakeholders** and complying fully and at all times with legal and regulatory requirements in relation to data protection and confidentiality. This policy sets out the data protection and confidentiality obligations and responsibilities of the Everton Family and how these will be met.

A definition of terms is included in section 18.

2 Scope

This policy applies to **all employees across the Everton Family**, this includes, Everton Football Club, Everton in the Community, Everton Ladies and Everton Free School.

The policy relates to **all personal information processed** across the Everton Family.

Deliberate, repeated or negligent breaches of this policy may result in disciplinary action up to and including **dismissal for gross misconduct**.

3 Reference Guides

Reference guides are easy-to-read, summarised versions on the key Policy principles and requirements. The reference guides associated with this Policy are:

- Consent Guidance Document
- Request for Information Guidance Document
- Breach Reporting Guidance Document

4 The UK General Data Protection Regulation

The General Data Protection Regulation (GDPR) came into force on 25th May 2018. It is a modernised, accountability based framework for data protection compliance through the European Union. The core concepts are much the same as in the Data Protection Act 1998 but enhanced in application and for organisations evidencing compliance.

When the UK left the European Union, the GDPR was converted into UK law, alongside an amended Data Protection Act 2018. The key principles, rights and obligations remain the same, however the UK has independence to amend the UK GDPR separate to the GDPR of the EU.

4.1 UK GDPR Principles

Principles have been a key aspect of data protection legislation; similarly, UK GDPR has 6 Principles. In summary these are:

Information must be:

- **Processed lawfully**, fairly and in a transparent manner
- Collected for specified, explicit and **legitimate purposes**
- **Relevant** and limited to the minimum necessary
- **Accurate** and up-to-date
- **Kept for no longer than is necessary**; taking into consideration legal retention obligations

- **Kept secure** from loss, damage destruction and unauthorised access

UK GDPR requires the Data Controller to be able to demonstrate compliance with the principles above. This **accountability** requirement means maintaining records, policies, procedures and risk assessments for processing activities.

4.2 Data Protection Officer

The Everton Family has a dedicated Data Protection Officer (DPO). The DPO is responsible for:

- **Informing and advising** the Everton Family about their data protection obligations.
- **Monitoring compliance** with data protection legislation, including **internal audit** activities, data protection **impact assessments** and **staff training**.
- Acting as the **point of contact** for supervisory authorities and Data Subjects, including staff, fans, pupils of Everton Free School and participants within Everton in the Community.

The Everton DPO can be contacted on:

Data Protection Officer
Everton Football Club
Goodison Park
Goodison Road
Liverpool
L4 4EL

Or

dataprotectionofficer@evertonfc.com

All staff should contact the DPO if they are unaware of their responsibilities or require any assistance in complying with the principles in this policy or associated guidance.

5 Processing Activities

To ensure compliance with data protection legislation, the Everton Family maintains a data mapping register. This records:

- **How** and **what** information is collected
- **Where** the information is stored
- **Who** has routine access to the information
- If the information is **shared**, **why and with whom**
- **How long** the information kept

All new or revised data flows must be notified to the DPO.

5.1 Lawful Basis

For the processing of personal data to be lawful, the processing activity must meet one of the following conditions under UK GDPR. In summary these are:

1) The **consent** of the individual has been obtained
2) The data is required for entering into or complying with a **contract with the Data Subject**
3) There is a **legal obligation** on the Data Controller to process the information
4) The data is required to **protect the life** of an individual
5) The data is required for a task in the public interest or for an **official function**

6) It is necessary for the **legitimate interests** of the Data Controller, considering the rights of the individual

For the processing of ***sensitive*** data to be lawful, one of the following conditions must be met ***in addition to the list above:***

1) The **explicit consent** of the individual has been obtained
2) The data is required to meet the obligations of **employment law**
3) The data is required to **protect the life** of an individual
4) The data is processed by a **not-for-profit organisation** relating only to members and not disclosed without the Data Subject's consent
5) The data has clearly been **made public** by the Data Subject
6) The data is required to exercise or defend **legal claims**
7) The data processing is in the **substantial public interest**, considering the rights of the Data Subjects
8) The data is required for direct **health care purposes**
9) The data is required for **public health** purposes, such as preventing the spread of infectious diseases
10) The data is necessary for archiving in the **public interest, scientific or historical research** purposes **or statistical purposes**, considering the rights of the Data Subject

Additional lawful basis purposing for personal and sensitive data is permitted under the Data Protection Act 2018, including:

1) Safeguarding of children and of individuals at risk
2) Anti-doping in sport
3) Standards of behaviour in sport
4) Equality

The lawful basis for each processing activity is recorded on the data mapping register.

5.2 Consent

The threshold for valid consent to process personal data has been strengthened under UK GDPR. Consent must be:

- A **positive action**, **prominent**, **freely-given** and **unambiguous**. Pre-ticked boxes are not adequate to show consent
- **Separate from other terms** and conditions
- **Clear** and **concise**

Consent means offering individuals real choice and control. There must always be the choice to withdraw consent and in the same manner in which it was obtained, for example **consent obtained on a website must allow consent to be withdrawn on the same website**.

Consent is just one of the processing conditions; other conditions may be more appropriate if valid consent is not possible, practical or applicable.

The Everton Family has a Consent Guidance Document to aid staff in complying with consent requirements; this guidance includes consent for marketing and obtaining consent of children in relation to online services. The guidance is available from the Everton Intranet.

6 Privacy Notices

Privacy notices, also known as Fair Processing Notices, inform individuals of how their data is processed and what rights they have. The information supplied to individuals must be:

- **Concise**, **transparent**, intelligible and **easily accessible**
- Written in **clear and plain language**; particular attention must be given to information addressed to children

UK GDPR stipulates what information must be made available; this depends on how the information is collected.

The Everton Family has adopted a tiered approach to privacy notices. There is a tier one notice for:

- Everton Staff, including volunteers and casual staff
- Pupils of Everton Free School
- Participants within Everton in the Community
- Fans, members and participants with Everton Football Club
- Academy Players

Tier one notices outline the general principles which apply to each group of Data Subjects and the processing of their data.

Tier two notices are created for each distinct processing activity. Each processing activity recorded on the data mapping register should be assigned a tier two notice where applicable. It is the tier two notice that will typically be provided to Data Subjects as they are concise, specific to each activity and to which rights apply to that processing.

Tier two notices are created in cooperation with the DPO who also maintains a central register.

In summary, a privacy notice must contain:

What information must be supplied?	Data obtained directly from Data Subject	Data not obtained directly from Data Subject
Identity and contact details of the Data Controller and DPO	✓	✓
Purpose and **lawful basis** of the processing	✓	✓
The **legitimate interests** of the controller or third party, where applicable	✓	✓
What data is being processed		✓
If and who the data is **shared with**; including whether the recipient is based **outside of the UK**	✓	✓
Retention period for the data	✓	✓
The **rights of the Data Subject**, including the right to withdraw consent where applicable	✓	✓
How to lodge a **complaint** with the Supervisory Authority	✓	✓
The **source** the personal data originates from and whether it came from publicly accessible sources		✓

Whether the provision of personal data is part of a **statutory or contractual requirement** or obligation and possible consequences of failing to provide the personal data	✓	
The existence of **automated decision making, including profiling** and information about how decisions are made, the significance and the **consequences**	✓	✓

Privacy notices need to be provided at **the time data is obtained directly from the Data Subject**. If it is obtained from another source, the notice needs to be provided to the Data Subject the earlier of within one month, at first communication of before the data is disclosed.

The Everton Family has a privacy notice Guidance Document to aid staff in complying with this requirement. The guidance document is available on the Everton Intranet.

7 Data Subject Rights

UK GDPR specifies the following rights for Data Subjects:

- Right to be **informed**
- Right of **access**
- Right to **rectification**
- Right to **erase** (typically known as "**right to be forgotten**")
- Right to **restrict** processing
- Right to **object** to processing
- Right to **data portability**
- Rights related to **automated decision** making and **profiling**

7.1 Right to be Informed

The right to be informed requires the provision of privacy notices to demonstrate fair, lawful and transparent processing.

7.2 Right of Access

Data Subjects have the right to access their personal data, subject to exemptions, regardless of the format in which the data is held. Requests must be resolved within one month, unless the request is complex or numerous. In such cases a further two months is permitted. **The DPO must approve all access requests when an extension is to be applied.**

Information should be provided in machine-readable electronic format wherever possible.

Access to information is free of charge, unless the request is a duplicate or the request is manifestly excessive. **The DPO must approve all access requests when a charge is to be applied.**

Prior to the disclosure of information, the Everton Family must take reasonable steps to confirm the identity of the requestor.

A Request for Information Guidance Document has been produced to aid staff in complying with requests; this guidance includes requests from 3rd parties such as relatives, solicitors and the Police. The guidance is available on the Everton Intranet.

7.3 Right to Rectification

The right to rectification allows a Data Subject to **amend data if it is inaccurate or incomplete**. If the Everton Family has disclosed information to a 3rd party which is inaccurate or incomplete, the 3rd party must be provided with the revised data.

Requests for rectification must be resolved within one month, unless the request is complex or numerous. In such cases a further two months is permitted.

If the Everton Family do not accept the rectification, this must be explained to the Data Subject. For example, the **Everton Family is not required to amend professional opinions or personal recollection of events**.

7.4 Right to Erase

The right to erase, commonly known as the right to be forgotten, is intended to allow a **Data Subject to have their information deleted** when there is no compelling purpose for it to be further processed.

This right only applies when:

- The purpose the data was collected for is **no longer relevant** to further retention
- The individual **withdraws consent**; if consent is the basis for processing
- The individual **objects to the processing** and there is no overriding legitimate interest for the processing to continue
- The personal data was **unlawfully processed** (i.e., it was processed in breach of UK GDPR).
- There is a **legal requirement** to erase the data
- The personal data is processed in relation to information society services **(online services) to a child.**

The right to erase in not absolute. The Everton Family **can refuse to comply** with a request for erasure if the personal data is processed for the following reasons:

- To exercise the right of **freedom of expression** and information;
- To exercise or defend **legal claims**
- To comply with a **legal obligation** or exercise official authority
- For **public health** reasons
- For **archiving in the public interest**, scientific research, historical research or statistical purposes;

Consideration must be given to whether the processing does cause damage or distress to the Data Subject; if this is the case it is likely to make the case for erasure stronger.

Requests relating to data processed when the subject was a child should also be carefully considered, as a child may not have been aware of the risks involved with processing at the time. The enhanced rights under UK GDPR for children strengthen requests to erase their data.

If the Everton Family does not accept the request to erase, this must be explained to the Data Subject. For example, the Everton Family will not delete safeguarding referrals or concerns, even when these were unfounded, if it is still within the documented retention period.

7.5 Right to Restrict Processing

The right to restrict processing is intended to allow disputes to be resolved without data being destroyed or further processed. The data is stored but no other activity is permitted whilst the restriction is in place.

A request for restriction can apply in the following circumstances:

- The **accuracy is contested** and processing is restricted until accuracy is verified
- Whilst determining whether an **objection** to processing is valid
- The processing was **unlawful but the Data Subjects opposes erasure**
- For the Data Subject to exercise or defend a **legal claim**

The Data Subject must be notified of the outcome to their request. The Everton Family is permitted to retain enough information about the individual to ensure that the restriction is respected in future.

7.6 Right to Object to Processing

Data Subjects have a right to object to processing which:

- Is **direct marketing**
- Is processed on the condition of **legitimate interests** or official authority
- Is processed for **scientific or historical research** and statistics

A direct marketing objection is an absolute right and must be actioned immediately.

The other objections require the Data Subject to demonstrate that the reason for their objection outweighs the Everton Family's purpose to process the data.

7.7 Right to Data Portability

Data portability allows a Data Subject to obtain their data in a manner which facilitates re-use across different services. If the individual requests this, then the data should also be transferred directly to another organisation if this is technically feasible. The timeframe for compliance is one month, with the option of a two-month extension for complex or numerous requests.

Data portability is more applicable with utility providers, credit cards and insurance companies rather than to the Everton Family, however a request could still be received.

The right to data portability only applies:

- To personal data the individual has **provided to a Data Controller**, not information the Data Controller has created
- If the processing is based on the **individual's consent** or for the performance of a contract
- If the processing is carried out by **automated means**.

7.8 Rights related to Automated Decision Making and Profiling

Profiling and automated decision making is decision making based solely on logic or algorithms without any human intervention; for example:

- Credit approval
- Recruitment aptitude tests with pre-programmed algorithm criteria

A Data Subject has the **right not to be subject to purely automated decision making which significantly affects them.**

Wherever profiling occurs, the Data Subject must:

- Be **informed** that profiling occurs

- Be allowed to request **human intervention** in decision making

For more information on profiling and automated decision making, see section 8.

8 Profiling and Automated Decision Making

Automated decision making is decision making without human intervention. Profiling is the use of that automated processing to evaluate an individual. Both are specifically restricted under UK GDPR.

For automated decision making and profiling to be lawful it must, in all cases:

- Have a documented **lawful basis**
- Be **notified** to the individuals
- Be explained how individuals can access their information which the automated decision is based on, and **correct any inaccurate data**
- Be explained that individuals **can object** to profiling
- Have **safeguards** to ensure the decision-making system is operating correctly

If the automated decision making has a significant legal effect, such as automated refusal of credit or declining a job application, the Everton Family is only permitted to undertake the activity when:

- The processing is necessary for entering into a **contract** with the individual, or
- The individual has provided **explicit consent**

Processing of special categories of data must have explicit consent unless substantially in the public interest.

Profiling activities must therefore:

- Be subject to a **Data Protection Impact Assessment** (See Section 9)
- Enable individuals to **request a human review** of the decision outcome

9 Data Protection Impact Assessments

A Data Protection Impact Assessment (DPIA) is a risk assessment of intended or current processing activities. It identifies how an organisation is compliant with data protection legislation and upholding Data Subject rights. DPIAs assist organisations in considering a range of options and implementing the most effective measures to safeguard information, including provisions to meet privacy by design and privacy by default. DPIAs are a new requirement under UK GDPR.

A DPIA is required when:

- Introducing **new technology**
- The processing poses **a high risk** to the rights of individuals; this includes large scale processing activities, large scale monitoring in public areas (e.g. CCTV) and profiling.

The Everton Family has a separate policy for DPIAs and the DPO can be contacted for advice and support.

10 International Transfers

GDPR is widely considered to be the most protective of Data Subject rights. Consequently, whenever personal data is transferred internationally, the Data Controller must be able to demonstrate that the protection offered to the individuals is not adversely affected as a result.

There are three main options which permit international data transfer. These should be considered in order:

1. Adequacy Decision

Countries outside the UK whose data protection laws are broadly similar to the GDPR can be assessed for Adequacy. This has previously been by the EU Commission; the UK has agreed to retain all adequacy decisions from the EU Commission in addition to granting the EU Adequacy.

Once Adequacy is granted, the country can be treated as though it is within the scope of the UK GDPR and no further safeguards are needed.

2. Appropriate Safeguards

In the absence of Adequacy, appropriate safeguards can be introduced to legally bind recipients of the data to uphold the information to a UK GDPR standard. Permitted appropriate safeguards are:

- **Binding Corporate Rules** – policies adopted by multinationals to transfer information within the organisation.
- **Standard Contractual Clauses** (model clauses) – A list of model clauses are approved for use by the Supervisory Authority to govern international transfers. The model clauses cannot be amended or altered. An assessment of local law compatibility with UK GDPR and the model clauses is still required.
- **Codes of Conduct or Certification** – Approved codes of conduct which companies can sign up to as a means of demonstrating UK GDPR-level compliance with personal data.
- **Ad-hoc clauses** – allow for the tailoring of standard clauses to meet a specific need. Ad-hoc clauses must be approved by a Supervisory Authority.
- **International agreement** – Legal agreement between two countries.

3. Derogations (for specific situations)

Derogations are exemptions to the prohibition of transferring personal data internationally. They apply in limited circumstances and with strict conditions. The derogations under UK GDPR are:

- If the **explicit consent** of the Data Subject has been obtained
- If the transfer of data is necessary for the **performance of a contract with the Data Subject** – this applies when there is no other way to fulfil a contract unless the data is transferred. This derogation is likely to apply for a player based outside the UK when signing for the Club. The only way to complete the contract is for the data to be sent between parties.
- Public Interest – data can be transferred if there is **substantial public interest**
- To exercise or defend **legal claims** (international litigations)
- Transfer of data from a **public register** – consultation with Data Subjects must give them the right to object.

The final derogation allows for **non-repetitive transfer concerning a limited number of Data Subjects who are informed** if a documented risk assessment has considered the protection of individual rights and the legitimate interests of the organisation.

For additional advice and support contact the DPO.

11 Children's Data

Many new protections to the processing of data relating to children are introduced under UK GDPR. UK law defines children, for data protection purposes, as 12 and under.

In summary the specific protections for children are:

- **Child friendly** privacy notices
- Online services offered to children with their consent must obtain the **consent of their parent**
- **Stronger justification** for requests to erase data if the data was obtained when the Data Subject was a child

The Everton Family has a Consent Guidance Document to aid staff in complying with consent requirements; this guidance includes consent for marketing and consent for children. The guidance is available from the Everton Intranet.

12 Data Processors

Data Processors are organisations acting on the instruction of the Data Controller in relation to the processing of personal information.

Whenever the Everton Family uses a Data Processor, it is a requirement under UK GDPR that a contract sets out the terms of processing. Contracts between Controllers and Processors ensure that both understand their obligations, responsibilities and liabilities.

Data Processor contracts must include:

- **Subject**, **duration** and **nature** of the processing
- **Purpose** of processing
- **Types** of personal data
- **Categorie**s of Data Subjects
- **Terms for the retention** and destruction of data
- **Obligations** and rights of the Controller
- For the **Processor to notify the Data Controller** of any personal data breaches
- **Obligations on the Processor** to assist the Data Controller in upholding Data Subject rights and in submitting to security audits
- For the Processor **not to use a sub-processor** without the prior written authorisation of the Data Controller.

The Everton Family will record all Data Processors on the data mapping register. Any planned or intended engagement with third parties must be notified to the DPO at the earliest opportunity and in all cases before any contract is entered into.

13 Remote Working

Remote working is any work-related activity away from the usual place(s) of work. This will include work from premises that are not owned or operated by the Everton Family (e.g. working from home) and may include staff working from the Everton Family premises if that is not a usual and expected part of their job role.

The following must be adhered to with all remote working:

- **Position yourself** to reduce the likelihood of unauthorised viewing of information; access to confidential information should be avoided wherever possible in public places or on public wi-fi.
- **Securely store manual records**; do not leave records on desks or otherwise unattended at any time.
- If you are unable to return manual records to your place of work, you must ensure they are **securely stored within your home/other location** and **returned to the office as soon as practically possible**. Secure storage includes a lockable drawer or cupboard and out-of-sight of unauthorised individuals. You must have line management approval to store any records at your home.
- When transferring manual records, they need to be **taken directly from location to location** with no records left unattended in vehicles; the only exception is for personal or vehicle safety and maintenance.
- Records must **never be left in vehicles overnight**
- Electronic data is only permitted to **be stored on the Everton Family approved storage media**; primarily this is Office365
- Data shall **not be stored on personal devices**, such as USBs or on personal computers. If an individual stores data on a personal device this may be considered a breach of the Everton Family's confidentiality and if applicable a breach of data protection legislation
- The Club's **Laptop Policy** and **Mobile Phone Policy** must be adhered to.

13.1 COVID and Working from Home

COVID-19 has resulted in a substantial proportion of staff working from home. Home working on a sustained basis presents unique data protection and information security risks. The following controls will help protect data when working from home:

- Protect your conversations from others in your household; you may need to wear headphones to prevent confidential conversations being overheard.
- To protect your own privacy, you may wish to blur your video background.
- Video calls should only be recorded if there is a necessity and after informing all parties; consent is not required but any objections should not unreasonably be rejected.
- The Everton Family should host all video calls when the subject is about Everton and its business. This is so that Everton maintain control over the security features, such as recordings, document shares and invitations. Meetings should be password protected or have "waiting room" turned on for guests.
- The use of external devices to record calls, such as recording a video from a mobile phone is prohibited.
- It is important that members are clear about who they are interacting with; use a photo and your real name.
- Be professional – ensure you are dressed appropriately, the surrounding are clean and clear, you have adequate lighting and volume. Maintain your focus on the call; close other windows

including email if this will be distraction. Enure you have logged out of calls fully before moving to another task.

14 Retention, Destruction and the Disposal of Equipment

The Everton Family has an Information Retention Policy to balance the rights of individuals and their information being kept for no longer than is necessary against the business and legal needs of the Everton Family.

All data should be retained for the minimum periods specified in the Information Retention Policy. At the end of the minimum period, if the data is no longer required it shall be securely disposed of.

Individual manual records must be disposed of in confidential waste. Bulk disposal needs should be notified to the IT department who will arrange the disposal.

Electronic data must be deleted when it is no longer required.

Equipment which stores data, such as laptops, mobile phones, CDs, USBs and medical devices must be notified to the IT department when they require disposal. The IT department will ensure that no data remains on the equipment.

Please see the Information Retention Policy for further details.

15 Data Breaches

A data breach is the unintended or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data that has a negative effect on the data. A personal data breach can be categorised broadly as a breach of security that has compromised the confidentiality, integrity or availability of personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data. Examples of data breaches include:

- Sending personal data to the wrong recipient, whether internal or external
- Access by unauthorised persons, including hacking
- Portable devices including USBs or laptops being lost or stolen
- Alteration to personal data without appropriate permission

Whenever a data breach occurs it is crucial that this is reported to the Data Protection Officer as soon as possible to allow investigation and prompt implementation of measures to minimise the impact of the breach.

15.1 Reporting Data Breaches

All staff have a responsibility to report a data breach at the earliest opportunity **and within one hour** of being aware of a breach, or likelihood of a breach.

Data breaches can be reported via the Data Breach Incident Form on the Intranet. The DPO can also be contacted directly if the intranet is not available.

The Everton Family has a Breach Reporting Guidance Document to aid staff in complying with this requirement. The guidance is available from the Everton Intranet. For additional advice and support contact the DPO.

15.2 Notification of Breaches

Data breaches are assessed by the DPO for severity, considering several factors including:

- The **number** of individuals affected
- The **sensitivity** of the information
- The **impact** of the breach on individuals
- Whether a **similar incident** has occurred recently

If the incident assessment identifies that there is a risk to the Data Subjects, the breach must be reported to the Supervisory Authority within 72 hours. If the full extent of the breach is unknown at this stage, it must still be reported with additional detail added later.

Notification to the Data Subjects should have a purpose, therefore under UK GDPR **notification to Data Subjects is required when there is a *high risk* to individuals**. One of the main reasons for informing individuals is to help them take steps to protect themselves from the effects of a breach. This may be because the data breach involves their financial details, other identifiers which could lead to identity theft or that the breach contains particularly sensitive information.

Formal notification to the Supervisory Authority and Data Subjects is the responsibility of the DPO. Notification from a customer service point of view to customers should be conducted in cooperation with the DPO.

15.3 Data Breach Reduction

A core component of data protection compliance is measures to safeguard information, reducing the likelihood of a data breach. There are many practical measures which must be followed such as:

- **Clear desk policy** – a clear desk policy aims to ensure that confidential information is not left unattended or in a manner in which it can be overseen by persons without a need to know.
- **Screens must be locked** when not in use (Ctrl,Alt + Delete or ⊞+L)
- **Manual records not left unattended**; they can be turned upside down when not actively in use
- **Do not share passwords** or usernames
- **Store electronic data on Office365** to ensure it is backed-up and secure
- **Report near misses and concerns** – a risky process can be investigated and changed before a real breach occurs
- **Training** – ensure awareness of responsibilities and update knowledge
- **Minimise data collection** – only collect the information that is required. The less information held, the lower the likelihood and severity of breaches

The Everton Family monitors staff usage of electronic systems for inappropriate use. This includes websites visited, where data is stored and what information is accessed. Indirect monitoring of individuals may also occur with CCTV and vehicle tracking as a consequence of the Everton Family tracking its assets. Monitoring information may be used for the prevention and detection of crime including theft and fraud.

16 Equality and Diversity

Everton Football Club is committed to being a leader in Equality & Diversity across all areas of its activity and for all stakeholders who engage with the Club. Non-compliance with legal and regulatory requirements in relation to Equality & Diversity is considered a material risk, is reflected in the Club's risk register and is mitigated through the allocation of specific resource to ensure compliance. Specific Equality & Diversity risks are regularly monitored through quarterly engagement by the Club's Risk & Assurance Manager with the Club's Equality & Diversity Lead. Material risks are escalated to the Club's Governance, Risk & Audit Committee to ensure they receive the appropriate level of scrutiny and where necessary resources are allocated to facilitate mitigation.

17 References and Associated Documents

The following should be read in conjunction with this policy

Policies

- Information Retention Policy – The Everton Family
- Data Protection Impact Assessment – The Everton Family
- Laptop Policy – The Everton Family
- Mobile Phone Policy – The Everton Family
- Acceptable Use Policy – The Everton Family
- Information Security Policy – The Everton Family

18 Definitions

Adequacy	A country determined by the UK or EU Commission or to have an equivalent level of data protection legislation to protect and promote the rights of Data Subjects.
Data Controller	Determines the purpose and means of processing. In effect the Data Controller is responsible for the data processing.
Data Processor	A Data Processor is responsible for processing personal data on behalf of a Data Controller.
DPO	Data Protection Officer. The lead person for data protection compliance within an organisation
Data Subject	The individual to whom the Personal Data relates.
Personal Information / Personal Data	Any information relating to an identifiable individual who can be directly or indirectly identified
Supervisory Authority	Regulators of data protection. For the UK this is the Information Commissioner's Office.
Sensitive Information / Special Categories	Data relating to: • race • ethnic origin • politics • religion • trade union membership • genetics • biometrics (where used for ID purposes); • health • sex life • sexual orientation