Worthing Town FC
Data Protection and Privacy Policy

1. Policy Objective and Scope

The objective of this policy is to direct the requirements for maintaining and improving good compliance with the Data Protection Act 2018and subordinate legislation, international standards and ICO codes of practice.

The scope of this policy is Worthing Town Football Club wide and applies to all officers, employees including directors; agency workers (i.e. temporary staff sourced from recruitment agencies); self-employed or contract workers; any individual on work experience (including interns); any individual training with Worthing Town Football Club under a contract; all employees of any outsourced providers; customers, operations, businesses and legal entities. For outsourced, joint venture or delegated operations, Worthing Town Football Club should satisfy itself as far as is risk, in line with the objectives set out in this policy.

Nothing is out of scope of this policy.

2. Policy Owner

- Policy Owner: Worthing Town Football Club Secretary
- Executive Sponsor: Director of Governance and Vice Chair

3. Risks

Failure to effectively control the uses of personal data could lead to financial and/or reputational exposure to the Worthing Town Football Club and/or its data subjects as a result of:

- Operational processing errors
- Personal date breaches
- Inability to meet data subjects expectations

The data protection and privacy controls developed by the Worthing Town Football Club are designed to comply with:

- The Data Protections Act 2018
- The EU General Data Protection Regulation (2016/679)
- The Privacy and Electronics Communications Regulations 2000 (PECR)
- The UK Information Commissioner's published Codes of Practice and guidance
- The applicable data protection laws and regulations of the jurisdictions in which Worthing Town Football Club operate, or data subjects reside.

4. Risk Appetite

- There is NO Tolerance for a breach of any specific requirements set out in this policy in sections 5 and 6 (below)
- There is NO Tolerance for a breach of this policy resulting in risk of a breach of data protection and privacy by employees, contactors, agents, directors of Worthing Town Football Club.
- Worthing Town Football Club has a LOW risk appetite for any activities that may constitute infringements of the rights and freedoms of data subjects under this policy and relevant data protection legislation.

5. Principles for Managing Data Protection Risks

- A data protection and privacy framework and awareness program in place that includes a written policy, guidance and instructions on processing personal data which conveys the expectations of the Board regarding data protection and privacy risk managements.
- Data protection and privacy risk exposure **MUST** be reviewed and assessed periodically by the Board to identify threats and mitigating actions.
- Appropriate measures and procedures **MUST** be in place to identify, report and record potential and actual events or breaches to the data protection team and corporate clients in compliance with statutory timeframes as set out un-Articles 33 GDPR.
- Appropriate measures **MUST** be in place to mitigate the likelihood of events and breaches and/or financial or reputational damage to the business and/or data subjects.
- Appropriate processes **MUST** be in place to record, report and investigate events/breaches in compliance with GDPR, to business managers, corporate clients, supervisory authorities and affected date subjects within time limits laid down by in Articles 33 and 34 GDPR.
- Appropriate processes and procedures **MUST** be in place for recording, reporting, and handling the rights of data subjects when exercised.
- An affective process is maintained for the quantification and recovery of actual data losses, including mechanisms to ensure effective coordination with the law enforcement agencies, other authorities, and corporate clients.
- An affective reporting process **MUST** be in place to track and disseminate information on potential or actual data protection events.
- A coordinated and independent approach to prioritise investigation and corrective actions **MUST** be in place to ensure data protection events and exercised rights are addressed in accordance with statutory times.
- All employees have an opportunity to escalate concerns about data protection and privacy confidentially and without detriment.

6. Essential Controls

Preventive

- All employees are subject to initial and ongoing screening and vetting of (set out under Worthing Town Football Club's Employment Screening and Security Vetting Policy).
- Security access controls in place for all premises, system and records.
- Segregation of duties between employees processing transactions, issuing payments/entitlements and preforming reconciliations.

- Verification of customer and caller identity when preforming transactions, updating account information or issuing payments/entitlements and periodic re-verification.
- Effective user access controls must be in place and monitored for all transactions involving personal.
- Records that contain personal data must only be held in proprietary approved systems and retained securely and confidentially.
- Customer due diligence undertaken on all customers before an ongoing business relationship is established with them.
- Supplier due diligence undertaken on all suppliers processing personal date on our behalf, before ongoing relationship is established with them an regularly thereafter.

Directive

- Ensure adequate skilled resources are in place to deliver effective controls for timely identification, assessment and reporting of data protection events and breaches.
- Mandatory employee awareness training in relation to data protection and privacy in each business area.
- Timely identification, reporting and provision of responses when data subjects exercise their rights under Data Protection Act 2018.
- Advice and guidance available to all staff, on all aspects of data protection and privacy via the Executive Owner.
- Data Protection by design and default **MUST** be incorporated into every project, material change to the design or delivery of a product or nay change of use of personal data held by any Worthing Town Football Club legal entity.

Detective

- Recording of all data protection events and breaches enables root cause analysis and discovery of trends for management MI.
- Recording of all activities in relation to data subjects exercising their rights under Data Protection Act 2018 enables appropriate management MI.
- Consistency of approach provided by the Executive Owner to requests for information made by law enforcement agencies ensure compliance with the data protection principles.

Corrective

- Referral of all data protection breaches of essential controls within the policy to the Executive Owner within 24 hours of becoming aware.
- All confirmed data protection events/breaches to be considered to identify whether additional controls are required to manage data protection risk within risk appetite.
- Regular management information and reporting in place to inform management on progress to remediate any identified date protection risks.

Any failure to comply with this policy and/or individual rights under the Data Protection Act 2018 must be notified to the Executive Owner immediately.

Disclosure of personal data and information to third parties must be managed in compliance with the Data Protection Act 2018, good practice as determined by the UK Information Commissioner's Office (ICO), corporate client instructions (where appropriate) and this policy.

Worthing Town Football Club is both a controller and a processor depending on the nature, scope context and purposes of processing. All processing activities involving personal data must be recorded and held by the Executive Owner in accordance with Article 30 GDPR.

Details of Worthing Town Football Club's responsibilities and liabilities as a controller for any processing of personal date and information carried out by the controller or the controller's behalf are set out in Worthing Town Football Club's Data Protection & Privacy Framework.

Details of Worthing Town Football Club's responsibilities and liabilities as a processor whenever personal data and information are process under contact to corporate clients are set out in Worthing Town Football Club's Data Protection & Privacy Framework

Where personal data and information is processed by another organisation on behalf of Worthing Town Football Club, there must be a contract evidenced in writing that sets out how the third part supplier complies with this policy, all required processes and procedures that must be followed to ensure that that processing is managed in compliance with data protection laws, good practice and Worthing Town Football Club's instructions.

7. Escalation of policy non-compliance

Anyone who identifies any instance of non-compliance with this policy, including any failure or weakness in applying the essential controls, must escalate the matter to the Executive Owner.

8. Waivers and Exceptions

It is not expected that waivers or exceptions to this policy will be required, other than in exceptional circumstances. Requests for dispensation against this policy should be made to the policy owner.

9. Policy Application and Responsibilities

In order to ensure that the data protection and privacy risk management standards, principles and control objectives set out above are achieved, responsibilities for apply to this policy are as follows:

Role	Key responsibilities
Worthing Town Football Club Board	• Set the tone and direction for effective data protection and privacy risk management and compliance . • Designated a Worthing Town Football Club Data Protection Officer • Review data protection and privacy risk appetite, tolerances and limits (in line with the Worthing Town Football Club risk management framework) • Review and approve changes to this policy. • Review management information on risk and control effectiveness. • Determine appropriate actions to remedy risk identified under this policy.
Directors	• Drive, monitor and co-ordinate Worthing Town Football Club's data protection and privacy risk management effectiveness.

	• Review policy, risk appetite and limits.
All employees (including contactors, agents etc.)	• To comply with the requirements of this policy. • General awareness of this data protection and privacy policy and the control objectives. • Understand their and responsibilities, and how their job functions and procedures are designed to manage any data protection and privacy risks under this policy. • Understand how non-compliance with policy and procedures may create an opportunity for data protection breaches to occur or go undetected, and the rights of data subjects to be ignored or not be met. • Ensure they complete all mandatory training and testing on data protection and privacy. • Report immediately any evidence of practices that indicate data protection or privacy breaches may have occurred either to line management or the data protection office in Compliance. • Escalate any instances of control weakness or failure.

10. Monitoring

Worthing Town Football Club is entitled to monitor electronic communications including telephone calls, email traffic sent and received (including content in certain circumstances) and the use of IT systems generally (including internet usage) without permission from the individual concerned:

- To check that they are business related or do not amount to excessive or unreasonable personal use.
- To check that they are generally in compliance with this policy.
- In order to assess the quality of service being given to clients and the effectiveness of Worthing Town Football Club's training.
- Where there are reasonable grounds to believe that criminal offences or breaches of Worthing Town Football Club's rules and procedures may be taking place.

If business needs dictate, Worthing Town Football Club will also check voice mailboxes and relevant IT systems in an employee's absence, including but not limited to unexpected or long term sick absence. In all of these above circumstances the relevant manager must contact the IT Service Desk to register their request. All such requests must include the written (email) authority of their manager.

11. Data protection and privacy framework

The data protection and privacy framework includes subordinate data protection policies, procedures, advice and guidance that support this policy and compliance with the Data Protection Act 2018.

Guidance on associated legislation will be published and maintained by the Data Protection Office as it becomes available from the supervisory authorities and Government.

12. Document Ownership & Control

Version History

Version	Effective Date	Author	Comments
1.0	5 April 2018	Simon Wadey	New policy compliant with DPA 2018