Information Security Management System Policy Statement

The purpose of this policy is to protect, preserve and manage the confidentiality, integrity and availability of information and all supporting business processes, systems and applications.

This policy sets out the principles required to protect Playfords information assets from threats, whether internal or external, deliberate or accidental.

This policy applies to, and is mandatory for, all Playfords personnel. All references made to **personnel** in this policy include Playfords employees, whether full or part-time, contractors and third-party personnel.

All personnel, regardless of their role, are responsible for conducting their work in a manner that protects the security of Playfords information. This includes adhering to the following information security principles:

- Information, and the supporting business processes, systems and applications, will be protected by implementing appropriate controls to preserve their confidentiality, integrity and availability.
- Risks to information will be actively identified and managed as per the Playfords Risk Management Framework and in context of the overall business risks.
- Physical and logical access to information is restricted to authorised users. The access to information will be monitored on an ongoing basis.
- Appropriate business continuity and disaster recovery plans are in place. The plans will be tested periodically.
- Third parties with authorisation to access Playfords information assets will be made aware of their responsibilities with regards to information security and the protection of information.
- Awareness of information security will be provided to all personnel on a regular basis.
- Information security incidents (both suspected and actual) will be reported immediately to the Networks Department or Quality & Information Security Manager.
- All personnel will comply with all relevant legal and regulatory requirements related to information security, including but not limited to the Data Protection Act 1998.
- Supporting information security policies are in place to ensure the principles above are achieved.

All Managers are directly responsible for implementing the policy within their business areas, and for adherence by their staff. It is the responsibility of each employee to adhere to the Information Security Management System Policy

This policy will be reviewed annually at The Management Review

Last reviewed Date
25th June 2014

ALAN TUOHY
Chairman