Restore
Harrow Green
Moving Professionals

Records Digital Datashred Relocation Technology

Information Security Policy

Policy Objective

Harrow Green and its subsidiaries will take all reasonable steps to protect its customers, its business partners and itself from security problems that might have an adverse effect on our operations or services and our professional standing.

Security problems can include confidentiality (people obtaining or disclosing information inappropriately) or integrity (information being altered or erroneously validated, whether deliberate or accidental).

We will:

•Use all reasonable, appropriate, practical and effective security measures to protect our important processes and assets in order to achieve our security objectives.

Information Security Objectives are:

•To continually review our use of security measures so that we can improve the way in which we protect our business.

•To protect and manage our information assets to enable us to meet our contractual, legislative, privacy and ethical responsibilities.

Responsibilities

All Harrow Green staff, past and present, permanent and temporary have an obligation to appropriately protect our information assets, systems and infrastructure. They will, at all times, act in a responsible, professional and security-aware way, maintaining an awareness of and conformance to this Policy. All suppliers and agents have the same obligations as stated in the policy scope.

Everyone will respect the information assets of third parties whether or not such protection is required contractually, legally or ethically. All staff are responsible for identifying security shortfalls in our existing security practices and/or improvements that could be made. These should be reported to senior management for appropriate action.

All management and supervisory staff are required to actively promote best practice amongst their supervised subordinates. The Managing Director has ultimate responsibility for ensuring that information within Harrow Green is adequately protected.

The Managing Director is responsible for ensuring that the stated objectives are achieved. Other individuals may be nominated and authorised by the Managing Director to pursue appropriate activities and actions that contribute to achieving our security objectives and that are consistent with this Information Security Policy.

The Managing Director will allocate sufficient resources so that Harrow Green can realistically achieve its security objectives. This includes people, time, equipment, software, education and access to external sources of information and knowledge.

Practices

We will identify and assess our security risks and their relative priorities, responding to them promptly and implementing safeguards that are appropriate, effective, and practical.

All staff, suppliers and agents will be responsible for their actions with regard to information security.

All information (including third party information) will be protected by security controls and handling procedures appropriate to its sensitivity and criticality. This may include but is not limited to appropriate access controls (via user ID and password protocols); revocation of access where information security is deemed to be at risk; central control of upload and use of software applications on company pc's; use of audit tools by administrators only, central control of system logs; secure control of remote login by SSL/VPN access controls. IT Administration will monitor activity to identify and appropriately act regarding use of unauthorised software or the introduction of malicious software to company systems (virus, Trojan etc.).

Data/Information must only be processed in accordance with Harrow Green's commitments under the Data Protection Act (1998 – and amendments to address the requirements of the EU General Data Protection Regulation (GDPR - 2018)), the Freedom of Information Acts (2000), The Privacy & Electronic Communications Regulations (EC Directive) Regulations (2003), The Electronic Commerce Directives (EC Directive) Regulations 2002, relevant copyright frameworks or other legislation which may apply.

All Harrow Green sites must exercise appropriate physical security controls to ensure visitor access is controlled and information available to visitors or the public is only accessible in accordance with this policy. Staff are responsible for the security of the equipment allocated to or used by them, and must not allow it to be used by anyone other than in accordance with this policy.

Where closed circuit television cameras and recording devices (CCTV) are utilised any data collected will only be processed in accordance with current codes of practice for the use of such equipment and will only be used, in the spirit of the Data Protection Act, "in the prevention of crime". Data will not be used to routinely monitor or review the normal activities of employees and visitors.

If given access to the e-mail system or to the internet, staff are responsible for the security of their terminals. If leaving a terminal unattended or on leaving the office they should ensure that they lock their terminal or log off to prevent unauthorised users accessing the system in their absence. Staff without authorisation should only be allowed to use terminals under supervision.

Desktop PCs and cabling for telephones or computer equipment should not be moved or tampered with without first consulting the IT Department.

Passwords are unique to each user and must be changed regularly to ensure confidentiality. Passwords must be kept confidential and must not be made available to anyone else. For the avoidance of doubt, on the termination of employment (for any reason) staff must provide details of their passwords to their Supervisor and return any equipment, key fobs or cards.

Staff who have been issued with a laptop, PDA or Blackberry or other smart phone must ensure that it is kept secure at all times, especially when travelling. Passwords must be used to secure access to data kept on such equipment to ensure that confidential data is protected in the event of loss or theft. Staff should also be aware that when using equipment away from the workplace, documents may be read by third parties, for example, passengers on public transport.

When needed, information may be made available outside of Harrow Green to other organisations in order to facilitate service provision. Information owners will be responsible for identifying to whom their information may be released and any appropriate level of encryption or other protection required. Harrow Green will develop effective Business Continuity and Disaster Recovery Plans to ensure that its activities can continue with minimal disruption, or other adverse impact, should it suffer disruption or security incident.

Data and information should only be deleted or (confidentially) disposed of in accordance with any retention requirements applicable to that information and by making reference to the information owner before destruction/deletion or disposal.

Actual or suspected security incidents will be reported promptly to the Managing Director who will manage the incident, and arrange for an analysis of the incident and consequent corrective and preventive actions.

Compliance with the Policy will be monitored and this policy reviewed, when appropriate, to describe new or improved practices to safeguard information security.

Policy Scope

This Policy applies to all individuals working at all levels and grades, including senior managers, officers, directors, employees, consultants, contractors, trainees, homeworkers, part-time and fixed-term employees, casual and agency staff. Third parties who have access to our IT and communication systems are also required to comply with this policy. Compliance with the Policy is mandatory and will form part of any contract of employment.

Failure to comply with the Information Security Policy could harm the ability of Harrow Green to achieve its aims and security objectives and could damage the professional reputation of the organisation and may, ultimately, be treated as a disciplinary matter which could result in dismissal

The Managing Director will be responsible for all decisions regarding the enforcement of this policy, utilising the disciplinary procedures at his or her disposal as appropriate.

Harrow Green will encourage the adoption and use of this Information Security Policy by third parties cooperating in joint ventures.

Signed on behalf of Harrow Green Limited

Nigel Dews - Managing Director