FLANNERY.

Flannery Plant Hire (Oval) Ltd,
Flannery House, Third Way,
Wembley, Middlesex HA9 0RZ
t: **020 8900 9290**
e: **info@flanneryplant.co.uk**
w: **flanneryplanthire.com**

IT POLICY

Version 1
1st November 2022

Contents

1. Introduction

Flannery Plant collects, processes, stores and uses information as part of its business processes. Information may be managed through computerised or manual systems. In all cases the Company needs to ensure that adequate controls are in place to ensure information is appropriately available, accurate, secure, and complies with legislative requirements. This information security policy provides management direction and support for information security across the Company.

The protection of individuals via the lawful, legitimate and responsible processing and use of their personal data is a fundamental human right. Flannery Plant is required to comply with the law governing the management and storage of personal data, which is set out in the Data Protection Act DPA 2018 (DPA) and the General Data Protection Regulation (EU Regulation 2016/679) (GDPR). For this reason, protection of personal data and respect for individual privacy is fundamental to the day-to-day operations of the business.

Flannery Plant is committed to compliance with all relevant UK and EU laws in respect of personal data, and to protecting the rights and freedoms of individuals whose information we collect in accordance with the GDPR and the DPA.

2. Legislation

This policy meets the requirements of the Data Protection Act DPA 2018 (DPA), the Copyright, Designs and Patent Act 1988, the Regulation of Investigatory Powers Act (RIPA) 2000, the Computer Misuse Act 1990 and the Counter-Terrorism and Security Act 2015 (which encompasses the 'Prevent' duty) General Data Protection Regulation (EU Regulation 2016/679) (GDPR).
This Policy should be read in conjunction with the Data Protection Policy and the Data Retention Policy and Schedule.

3. Aim of Policy

The purpose of this Policy is to minimise operational damage by reducing the impact of security incidents and ensure business continuity. The policy will provide a framework for use of Flannery Plant IT resources.
This policy will demonstrate how the Company will manage information security, provide guidance to users, administrators and developers of information systems and the controls in place to maintain the integrity of information.

Compliance is overseen by the Directors, IT Department and the appointed Data Protection Officer (DPO).

4. Scope

This policy applies to all Flannery Plant employees, consultants, contractors and operatives. This policy relates to all IT-related systems, hardware, services, facilities, and processes owned or otherwise made available by Flannery Plant or on its behalf. All employees and third parties are expected to comply with this policy, failure to do so, may lead to disciplinary action, dismissal, or termination of contract.

5. Key Responsibilities

- Senior Management / Department Heads
  - Directors have an overall responsibility for ensuring that the organisation complies with its legal obligation in relation to the handling of personal data.
  - Provide the necessary support to the IT Department, review and implement new IT systems suggested by the IT Manager and IT Department.
  - Ensure relevant IT training has been provided to all levels.

Registered in England No. 1058421 | VAT Registration No. 236 2899 34

- Responsible for implementing the policy within their business areas and for adherence by their team.
- Report any breaches to the IT Manager/DPO and Compliance Manager.

➢ IT Manager / Data Protection Officer (DPO)

- Responsible for monitoring internal compliance.
- Review and implement new IT Systems.
- As with other considerations including Quality and Health & Safety, Information Security aspects are taken into account in all daily activities, processes, plans, contracts and partnerships entered into by the company.
- Review and update policies and procedures for the IT Department.
- Ensure all employees are instructed in their security
- Briefing the Management on Data Protection responsibilities.
- Handling Subject Access Requests
- Approving unusual or controversial disclosures of personal data
- Reviewing and approving contracts with internal and external Data Processors.
- Inform and advise Flannery employees of their data protection obligations.
- Provide information and advice and act as a main point of contact.
- Report any breaches to Senior Management and Compliance Manager.
- Report serious incidents to the Information Commissioner's Office (ICO).

➢ Employees

- All employees must read, understand, and accept any policies and procedures that relate to the personal data they may handle during their employment and day-to-day activities at Flannery Plant.
- Responsible for collecting, storing, and processing any personal data in accordance with this policy.
- All employees should treat company's property, whether material or intangible, with respect and care.
- Report any breaches to the IT Manager or their Line Manager.

6. Information Handling

6.1. Classification of Information

An inventory will be maintained of all the Company's major corporate IT assets and the ownership of each asset will be clearly stated. Within the inventory, the information processed by each I.T. asset will be classified according to sensitivity.

6.2. Disposal of Equipment

When permanently disposing equipment containing storage media, all sensitive or confidential data and software must be irretrievably deleted by using an in-house procedure or by another licensed organisation.
Damaged storage devices containing sensitive or confidential data will undergo assessment to determine if the device should be destroyed, repaired, or discarded. Such devices will remain the property of Flannery Plant and only be removed from site with the permission of the IT Department.

6.3. Disposal of Information

Any paper documents with a classification of sensitive or above must be shredded.
Sensitive or confidential information must not be kept in a cloud storage service which is not approved by the company.
Redundant equipment including storage devices, are disposed of by approved suppliers who securely wipe and recycle the hardware

6.4. Precautions against hardware, software, or data loss

Equipment must be safeguarded appropriately, especially when left unattended. Files downloaded from the internet, including files attached and links within email, must be treated with caution to safeguard against Phishing type attacks for both malicious code and the harvesting of personal information.

6.5. Working Practices

The company encourages a clear screen and clear desk policy particularly when employees are absent from their normal desk and outside normal working hours. Employees should log out or lock their workstations when not in use. In addition, screens on which sensitive or confidential information is processed or viewed should be fitted with a privacy filter or be sited in such a way that they cannot be viewed by unauthorised persons.

6.6. Backup and recovery

The IT Department ensure that tested backup and system recovery procedures are in place. Backup of the Company's information assets and the ability to recover them are important priorities. The IT Department must also ensure that safeguards are in place to protect the integrity of information during the recovery and restoration of datafiles; especially where such files may replace files that are more recent.

6.7. Archiving

The archiving of information must take place with due consideration for legal, regulatory and business issues, with liaison as needed between IT department, records managers and data owners, and in line with the Data Retention Policy. Storage media used for the archiving of information must be appropriate to its expected longevity. The format in which the data is stored must also be carefully considered, especially where proprietary formats are involved.

6.8. Sensitive or Confidential Information

Sensitive or confidential data may only be transferred across networks, or copied to other media, when the confidentiality and integrity of the data can be reasonably assured and in accordance with the company's Data Protection Policy. Sensitive or confidential data should only be accessed from equipment in secure locations and files must never be printed on a networked printer that does not have adequate protection or security.

6.9. Use of electronic communication systems

The identity of online recipients, such as email addresses and fax numbers should be checked carefully prior to dispatch, especially where the information content is sensitive or confidential. Information received electronically must be treated with care due to its inherent information security risks. File attachments should be scanned for possible viruses or other malicious code. Sensitive or confidential information should only be sent electronically (e.g. by e-mail) to external recipients when it is encrypted or protected by a password.

6.10. Access to personal or individual data for systems management purposes

Some individuals may need access to personal data identifying individuals, or to data which belongs to others, in order to manage systems or to fix problems. These individuals will be required to sign a data protection declaration before they are sanctioned to carry out these duties.

6.11. Information life cycle management

All users of information systems must manage the creation, storage, amendment, copying and deletion or destruction of data files in a manner which safeguards and protects the confidentiality, integrity, and availability of such files. Day to day data storage must ensure that current information is readily available to authorised users. Any archives created must be accessible in case of need.

Registered in England No. 1058421 | VAT Registration No. 236 2899 34

7. General Use / Network Access

Where a Company device has been provided, users will be granted access to Company Applications, Shared File Locations and other Tools or Utilities to carry out their role and responsibilities. Use of Company equipment should be for the sole purpose of carrying out your role and is not intended for personal use. Access to personal e-mail accounts, cloud locations, or other public systems is not permitted and poses a security risk. Any breach of this can result in disciplinary action.

Steps have been taken to ensure you have adequate permissions, but where a user may have not been given access to a system or resource, they require then the request must be made to their Line Manager who will in turn approve for the IT Department to implement. Similarly, where a user's role may change or may have access to a resource that is no longer required, then this must be made aware to the IT Department to update.

8. Personal use of mobile phones at desk

Employees must leave phones in a desk drawer, coat/bag, or a company locker and have their phone set to silent or vibrate. Any essential calls or texts must be made away from their desk in a private area and phones must not be made during meetings.

9. Passwords

Flannery Plant have a password policy enforced for active directory and Office 365 accounts. This policy should also be used as a guide for other accounts and services where a policy cannot be enforced.

Passwords must meet the following requirements:

- not match one of the previous 3 passwords
- must be changed every 90 days
- must be a minimum of 8 characters long
- contain at least one number and one special character
- not contain the user's account name or parts of the user's full name that exceed 2 consecutive characters

10. Internet Access

Use of the internet is permitted and encouraged where such use supports the goals and objectives of the business.
However, Flannery Plant has a policy for the use of the internet whereby employees must ensure that they:

- comply with current legislation
- use the internet in an acceptable way
- do not create unnecessary business risk to the company by their misuse of the internet

The following is deemed unacceptable use or behaviour by employees:

- visiting internet sites that contain obscene, hateful, pornographic or otherwise illegal material
- using the computer to perpetrate any form of fraud, or software, film or music piracy
- using the internet to send offensive or harassing material to other users
- downloading commercial software or any copyrighted materials belonging to third parties, unless this download is covered or permitted under a commercial agreement or other such licence

Registered in England No. 1058421 | VAT Registration No. 236 2899 34

- hacking into unauthorised areas
- publishing defamatory and/or knowingly false material about Flannery Plant, your colleagues and/or our customers on social networking sites, ‘blogs’ (online journals), ‘wikis’ and any online publishing format
- revealing confidential information about [business name] in a personal online posting, upload or transmission - including financial information and information relating to our customers, business plans, policies, staff and/or internal discussions
- undertaking deliberate activities that waste staff effort or networked resources
- introducing any form of malicious software into the corporate network

If you produce, collect and/or process business-related information in the course of your work, the information remains the property of Flannery Plant. This includes such information stored on third-party websites such as webmail service providers and social networking sites, such as Facebook and LinkedIn.

Flannery Plant accepts that the use of the internet is a valuable business tool. However, misuse of this facility can have a negative impact upon employee productivity and the reputation of the business. In addition, all of the company's internet-related resources are provided for business purposes. Therefore, the company maintains the right to monitor the volume of internet and network traffic, together with the internet sites visited. The specific content of any transactions will not be monitored unless there is a suspicion of improper use.

Where it is believed that an employee has failed to comply with this policy, they will face the company's disciplinary procedure.

11. Remote Access

It is the responsibility of Flannery Plant employees, contractors, vendors and agents with remote access privileges to our corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection. General access to the Internet for recreational use through our company network is strictly to our employees, contractors, vendors and agents (Authorised Users). When accessing our network from a personal computer, Authorised Users are responsible for preventing access to any company computer resources or data by non-Authorised Users.

Performance of illegal activities through our company network by any user (Authorised or otherwise) is prohibited. The Authorised User bears responsibility for and consequences of misuse of the Authorised User’s access. Authorised Users will not use our networks to access the Internet for outside business interests.

Secure remote access will be strictly controlled with encryption through our Virtual Private Networks (VPNs)) and strong pass-phrases. Authorised Users shall protect their login and password, even from family members.

While using our corporate owned computer to remotely connect to our corporate network, Authorised Users shall ensure the remote host is not connected to any other network at the same time, with the exception of personal networks that are under their complete control or under the complete control of an Authorised User or Third Party.

Use of external resources to conduct company business must be approved in advance by the appropriate business unit manager.

All hosts that are connected to our company’s internal networks via remote access technologies must use the most up-to-date anti-virus software this includes personal computers.

Personal equipment used to connect to our company’s networks must meet the requirements of company owned equipment for remote access - and approved by your business unit leader.

Registered in England No. 1058421 | VAT Registration No. 236 2899 34

The IT Department will verify compliance to this policy through various methods, including but not limited to, periodic walk-throughs, video monitoring (if applicable), business tool reports, internal and external audits, and/or inspection. The results of this monitoring will be provided to the appropriate business unit manager.
An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment

12. Clean Desk Policy

Users are required to secure all sensitive/confidential information in their workspace at the conclusion of the workday and when they are expected to be away from their workspace for an extended period of time. This includes both electronic and physical hardcopy information.

Computer workstations/laptops must be locked (logged out or shut down) when unattended and at the end of the workday. Portable devices like laptops and tablets that remain in the office overnight must be shut down and stored away.

Mass storage devices such as CD, DVD, USB drives, or external hard drives must be treated as sensitive material and locked away when not in use.

Printed materials must be immediately removed from printers or fax machines. Printing physical copies should be reserved for moments of absolute necessity. Documents should be viewed, shared and managed electronically whenever possible.

All sensitive documents and restricted information must be placed in the designated shredder bins for destruction or placed in the locked confidential disposal bins.

File cabinets and drawers containing sensitive information must be kept closed and locked when unattended and not in use.

Passwords must not be written down or stored anywhere in the office.

Keys and physical access cards must not be left unattended anywhere in the office.

Repeated or serious violations of the clean desk policy can result in disciplinary actions.

If you notice that any of your devices or documents have gone missing, or if you believe your workspace has been tampered with in any way, please notify DPO immediately.

13. Training

Training on the company's IT systems will be provided by the IT Department and/or Line Managers within the first couple of weeks a new starter joins the company.

14. Compliance

The IT Department will verify compliance to this policy through various methods, including but not limited to, periodic walk-throughs, video monitoring (if applicable), business tool reports, internal and external audits, and/or inspection. The results of this monitoring will be provided to the appropriate business unit manager.

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Registered in England No. 1058421 | VAT Registration No. 236 2899 34

15. Related Policies and Procedures

Disaster Recovery Plan (DRP)
Data Retention Policy and Schedule
DSE Policy
Home and Remote Working Policy
Privacy Policy
Mobile Phone Policy

16. Implementation and Review

Copies of the policy will be provided to all individuals and the receipt acknowledgment by each person shall be maintained. Flannery's will communicate, implement, and maintain this policy at all times throughout the organisation.

This policy is effective from the 1st November 2022 and will be reviewed annually. Overall implementation of this policy lies with Patrick Flannery (Managing Director) and Rob Gaubert (IT Manager). Any queries relating to this policy should be directed to IT Manager in the first instance.

Patrick Flannery
Managing Director

1st November 2022

This is a controlled document. Whilst this document may be printed, the electronic version is the controlled copy. Any printed or saved copies of the document are not controlled.

Registered in England No. 1058421 | VAT Registration No. 236 2899 34