Acceptable Use Policy and Agreement

Version 1.2

Date of issue: 18/05/2018
Last Revision: 17/08/2018

1. The Policy

Ogilvie Group is committed to complying with data protection legislation, the EU General Data Protection Regulation (GDPR), and data protection best practice.

The Acceptable Use Policy and Agreement provides employees, contractors, suppliers, stakeholders or other third parties with clear rules and guidelines on how to remain compliant with these requirements when working at both Ogilvie Group locations and remotely.

2. Policy in Operation

2.1 Acceptable Use of Assets

Information assets may be used only for carrying out **Ogilvie Group** activities.
Definition: Information asset – an information asset is a body of information, defined and managed as a single unit so it can be understood, shared, protected and exploited efficiently.

Each employee is responsible for safeguarding their **Ogilvie Group** issued equipment (e.g. laptops) and must immediately report to the service desk if the security of the device is compromised including loss or theft of the device.

Users may not visit Internet sites that contain obscene, hateful, illegal or other inappropriate (including online gambling) material, and shall not make or post indecent remarks, proposals or materials on the Internet or company equipment.

It is prohibited to use information assets in a manner that unnecessarily uses capacity, weakens the performance or poses a security threat. Users may use the information asset only for purposes for which they have been authorised and must not take part in activities which may be used to bypass information security controls.

It is specifically prohibited:

1. To access **Ogilvie Group** internal networks with any devices that are not authorised devices

2. To download images or video files or any other files which do not have a business purpose, send E-mail chain letters, play games, etc.

3. To install software on a local computer without explicit permission from IT

4. To use cryptographic tools (encryption) on a local computer, except in the cases outlined by the Information Security policies and procedures.

5. To install or use peripheral devices such as modems, memory cards or other devices for storing and reading data (e.g. USB flash drives) without explicit permission by the approved line manager and IT.

2.2 Backup Procedure

Employees, contractors, suppliers, stakeholders or other third parties must store working information on Ogilvie Group drives where possible and not use or store data on local hard drives. Where a situation dictates you must store information locally, this information must be encrypted and transferred to the appropriate Ogilvie Group network location at the next available opportunity.

Date	Version	Document Revision History	Document Author/Reviser
18 May 2018	1.0	Document Creation	Debra Cairns
7th August 2018	1.1	Document Review	John Watson
17th August 2018	1.2	Document Approved	John Watson

2.3 Removable Media Policy

Removable media poses severe security risks for **Ogilvie Group** and users need to fully consider the consequences of information being lost or wrongly disclosed through these technologies. Removable media is the term used to describe any kind of portable data storage device that can be connected to and removed from your computer. Examples include floppy disks, CDs, DVDs, USB memory sticks/pens and portable/zip hard drives.

Critical user guidelines are:

- Storage on removable media must be temporary in nature
- The media must be secured in a locked container/ filing system when unattended
- Confidential or sensitive materials must be stored on the devices encrypted and password protected.

2.4 Device Screens

If the authorised employee, contractor, supplier, stakeholder or other third party is not at their workplace then devices should be locked or logged off when not in use, and where appropriate, stored securely.

3.5 Mobile Computing

Special care should be taken when mobile computing equipment is placed in cars or other forms of transportation, public spaces, hotel rooms, meeting spaces, conference centres, and other unprotected areas outside **Ogilvie Group** premises. Employees, contractors, suppliers, stakeholders or other third parties taking mobile computing equipment off-premises must follow these rules:

- Mobile computing equipment storing important, confidential or critical information must not be left unattended and, if possible, should be physically locked away in a secure location

- When using mobile computing equipment in public places, take care to ensure data cannot be read by unauthorised persons

- Access corporate files via VPN utilising two factor authentication and avoid storing files locally whenever possible

- 'Strictly Confidential' information on mobile computing devices must be password protected with a strong password

- Ensure Confidential and Strictly Confidential information is stored on mobile computing devices that are encrypted.

4. Continual Improvement

The Acceptable Use Policy and Agreement relates to the Information Security Policy and will be continually reviewed to ensure its effectiveness is maintained. This will include:

- An annual review of the Policy, or when a significant change is made to the systems, people or processes related to this policy.

5. Roles & Responsibilities

5.1 Overall Ownership of the Acceptable Use Policy and Agreement

Ultimate responsibility for the Acceptable Use Policy and Agreement rests with the **Ogilvie Group Board and Data Protection Representative (DPR)**, but on a day-to-day basis the Head of IT shall be responsible for managing and implementing this policy and related procedures. Other day to day tasks of the Head of IT Include:

- Reporting to other members of the **Ogilvie Group Board and Management Team** the state of IT security and potential and confirmed Information Security Incidents within the organisation.

- Maintaining a current copy of the **Ogilvie Group** Acceptable Use Policy and Agreement (this document) and ensuring it's availability to staff, stakeholders and interested parties.

- Ensuring all staff are aware of their responsibilities under the Acceptable Use Policy and Agreement.

5.2 Responsibilities of All Staff

All staff must be aware of **Ogilvie Group's** Acceptable Use Policy and Agreement and their responsibilities. In addition, all staff should ensure the following is adhered to:

- All confirmed or suspected Information Security Incidents related to the Acceptable Use Policy and Agreement are reported immediately to the appropriate appointed individual:

  - Line Manager, Information Security Manager/ Information Technology Manager or Data Protection Representative (DPR)

- Any concerns relating to the Acceptable Use Policy and Agreement and Procedures are reported immediately to the appropriate appointed individual:

  - Line Manager, Information Security Manager/ Information Technology Manager or Data Protection Representative (DPR)

It is vital that all employees carefully read the Acceptable Use Policy and Agreement and understand how this pertains to their position. If anything is not clear or understood it is the employee's responsibility to request clarification from their manager.

Failure to comply with this Acceptable Use Policy and Agreement may constitute a disciplinary matter in line with the **Ogilvie Group Disciplinary Procedures (HR)**.

6. Additional Information

This Policy document will be reviewed regularly and updated as necessary. However, it will only be re-issued to all Staff when there is a significant change to the Policy or Procedures. The current version of the document can be obtained from **Group HR**.

7. Acceptable Use Agreement

I accept that I have been granted the access rights defined in this policy to **Ogilvie Group** information assets and systems. I understand and accept the rights which have been granted, I understand the reasons for these access rights, and I understand that breach of them, and specifically any attempt to access services or assets that I am not authorised to access, may lead to disciplinary action and specific sanctions in line with **Ogilvie Group Disciplinary Procedures (HR)**.

I understand that failure to comply with this Policy and Agreement, or the commission of any information security breaches, may lead to the invocation of the **Ogilvie Group Disciplinary Procedures (HR)**.

I acknowledge that I have received adequate training in all aspects of my use of **Ogilvie Group** systems, physical assets, information assets and Information Security Management System (ISMS) Policies and Procedures as well as my responsibilities under this agreement.

8. Document Owner and Approval

The Head of IT is the owner of this document and is responsible for ensuring that this procedure is reviewed in line with the review requirements of Data Protection Regulations. A current version of this document is available to all members of staff on the Group Intranet.

John F. Watson
Group Financial Director

17th August 2018