Monitor Group Information Security Policy

1. The Purpose of this document

● To set guidelines and procedures to secure, protect, and manage the information required to conduct business by Monitor Group

● To set guidelines for all employees involved in any computer based activity, the use of software applications and/or the processing of data belonging to and held by Monitor Group

● To define the tools and methods used to secure information held by Monitor Group

● To state that the company relies on computer based systems and expects all employees to manage data in a confidential and secure way

● To state that all employees must adhere to the company policies and not disclose to any other party or make personal use of the private information of the company

2. The Scope of this document

● This document applies to all employees of Monitor Group at all times and whether located within the physical offices or not

● The document applies to all information held by Monitor Group and all information technology systems utilised by Monitor Group

3. Where is our Data held?

Monitor Group recognises the value of cloud-based file storage systems both to data security and data accessibility. The system we use is Datto Backup

This system is only accessible by our external I.T consultants. This is secured by a 2 step authentication process and can only be accessed at our request by Chris Verbiest at Verbo Computers, Lion House, 100 High Street Newington, Sittingbourne Kent ME9 7JH. All confidential or personal information held by Monitor Group should only ever be stored in this location.

Monitor Group also provides additional storage options for its employees such as standard hard-drive memory on PCs and Laptops and removable media such as memory sticks. Information stored in these locations is considered unsecured and as such should not contain any confidential or personal information. It is the employee's responsibility to comply with these guidelines. Data may also be held on our email exchange server – Microsoft Office 365. More details on this can be found in the Transfer of Data section below.

4. Transfer of Data

Monitor Group employees may transfer personal information to authorised recipients using our email system – Microsoft Office 365. Each email account is accessible only via unique usernames and passwords distinct to individual employees. Data held on Microsoft Email accounts is stored in dedicated server space in either the UK, EU or US. Microsoft are

signatories to the EU-US Privacy Shield Agreement and have confirmed that they are compliant with all UK and EU regulations on data protection.

5. Removeable media

Monitor Group also provides additional data storage options for its employees such as standard hard-drive memory on PCs and Laptops and removable media such as memory sticks. From time to time it may be necessary for data to be transferred using these devices. Removeable media should only be used in specific circumstances and with the permission of a senior manager of Monitor Group. Data stored on removeable media remains the responsibility of the employee at all times. Once the need for that data to be transferred has expired, the data should immediately be deleted.

6. BYOD – Bring Your Own Device

Monitor Group discourages the use of personal devices to process company data. Any employee with a regular need to use additional devices should inform their line manager and a company device will be provided. Monitor Group also recognizes the need for flexible data solutions and that on occasion it may be appropriate for personal devices to be used. This should only be in specific circumstances and with the express permission of a senior manager of Monitor Group. The most common examples of this will be the Microsoft Outlook app. Once the need for the use of these on personal devices has expired, then the apps and all associated data should be deleted.

7. Physical security

All data held in the Monitor Group office whether electronically or paper-based is protected by a number of physical security measures. Monitor Group offices are accessed only via a lockable door and the issuing of keys is limited to senior staff only or access to the building is via a key code which is changed at least once per year. The key code should never be given to anyone who is not a permanent Monitor Group employee. Outside of office hours all offices are kept locked and secured by a key code burglar alarm. Security cameras are also installed at all locations.

8. Electronic security

Data transferred in and out of the building is controlled and protected via a sophisticated firewall system which sits between us and our ISP. This system is provided and maintained by our external I.T consultants, Verbo Computers. More details can be provided upon request. All Monitor Group computers are further protected by a managed anti-virus and anti-malware system. This is provided and maintained by our IT provider. We provide Wireless internet access within our office building however this availability is password protected and limited to standard office hours only.

9. Password policy

All Monitor Group passwords are covered by the same password policy. This states that all passwords must be:

- Private
- Unique
- Never written down
- Be at least 8 characters in length

● Contain a combination of letters and numbers

● Replaced when compromised

In certain circumstances, such as sickness or holiday, employees may be required to share their passwords with their line manager. In no circumstances should the passwords be shared with anyone else.

10.Acceptable Personal Use

All Monitor Group employees should be aware that all systems, data and equipment are provided for use in line with company activities only. Reasonable personal usage during lunch and breaktime is permitted however this is a benefit that may be removed at any time should it be abused. Employees should be aware that the company operates a security filter over its internet connection and many inappropriate sites will be blocked. Under no circumstances should such facilities be used for personal financial gain, to solicit others for activities unrelated to the organisation's business, or in connection with political campaigns or lobbying. The organisation's tools cannot be used at any time for defamatory or obscene material, to infringe another person's intellectual property or to violate any laws. You acknowledge and accept that the Company may monitor electronic correspondence (including email, voice and text messages), which you receive at work in order to ensure the integrity of its information technology or to prevent or detect criminal behaviour, or behaviour, which contravenes employment legislation or other Company policies.

11. Social Media

Monitor Group utilises several social media accounts and encourages the use of social media by its employees to promote the services of the company. Employees should be aware that personal social media accounts used for company business should always reflect the company's values, ethics and codes of conduct and should never be used for the transfer of personal information. This policy applies to all social media accounts which make reference to Monitor Group.

12. Software Downloads

Whilst the use of internet downloaded software is an essential component of any business, it also comes with inherent risks. All software downloads should be signed-off by a senior manager before they are commenced. Monitor Group may require employees to remove software downloaded on to company machines without permission.

13. Clear desk – Clear screen

To minimize the loss or unauthorised access of personal information, Monitor Group operates a Clear Desk – Clear Screen policy. This means that all paperwork containing personal information should be locked away whenever the employee is away from their desk for an extended period of time. Lockable cabinets will be provided to all employees to facilitate this. Documents should never be saved to the desktop and computer screens should always be locked whenever the employee is away from their desk for an extended period of time.

14. Support Functions

Monitor Group has taken the decision to outsource all IT support functions. In the event of any issues or problem with either equipment, systems or data, please follow the below reporting lines:

Data Breach - Any suspected data breach should be reported immediately to your line manager or, if not available, then an alternative senior member of staff.

Network infrastructure, internet connectivity, physical security - These services are all provided by Verbo Computers and any problems should be reported immediately to Chris Verbiest or Craig Dexter.

Operating system, software, PCs and Laptops - All of the above services are provided under our Managed Support Package provided by Verbo Computers. They can be contacted directly on 01474 353277

15.Data Destruction and Deletion

As part of our Data Management procedures and to ensure compliance with GDPR we will conduct a regular Data Deletion Process each year. At this point we will review all data held and delete as per the timescales required by law.

All computer hardware will be destroyed when no longer required and all data deleted in line with CESG approved methods. A Data Destruction certificate will be obtained and kept on record.

16. Action resulting from a breach in this policy

Employees are expected to adhere to this policy at all times and Managers are expected to enforce it. Failure to adhere to this policy may result in disciplinary action.

17.Alteration to this policy

This policy will be subject to regular review and will be updated to reflect changing legislation and the changing needs of the business itself. Any revisions will be re-issued to all employees at that point.

Last updated: 10th November 2024 **Next Review November 2025**

Approved by: Angus Henry MD