The Groves Medical Group

The Groves Medical Group
171 Clarence Avenue,
New Malden,
Surrey, KT3 3TX

Cyber Policy

Version Control

Version:	1.0
Date of version:	6th November 2018
Author:	Steven Davies
Approved by:	
Confidentiality level:	Internal

Amendment History

Date	Version	Author	Details of Amendment

Introduction

This policy applies to The Groves Medical Group and where appropriate to third parties, consultants, contractors and suppliers that have access to The Groves Medical Group systems and technology. It is one of the supporting documents that makes up the Information Security Policy.

Policy Statement

Providing an efficient and secure cyber environment is critical to the overall goals of maintaining information security throughout The Groves Medical Group and its dealings with clients, suppliers, contractors and employees. The Groves Medical Group takes a number of steps to ensure that risks of loss, theft or corruption of electronic information are minimised, and should any incident occur, it is dealt with professionally, quickly and steps are put in place to prevent a recurrence.

The Executive Board (which includes the CEO and COO) is committed and supportive of the steps required to manage and safeguard the data and systems used to process data and understands that maintaining high standards of Cyber Security is a key attribute that will underpin the long-term future of The Groves Medical Group.

Responsibility for information security lies with all staff, but management play a key role in ensuring the implementation of this Policy.

Scope

This Cyber Policy is designed to protect electronic data used by The Groves Medical Group but in particular that of any customer. In assessing the risks, which in turn dictate the necessary controls, the following are considered.

- Loss or theft of data or assets
- Reputational damage to The Groves Medical Group or the customer
- Ability to maintain service levels
- Fraud
- Privacy breach
- Accuracy of data

This Policy is implemented through a number of controls and procedures that are documented elsewhere as part of the overarching Information Security Policy. What follows is a summary of the controls in place.

Safeguards

The following high-level groups of safeguards are in place to minimise the risk of cyber-attacks and maintain a good level of cyber security.

Risk Assessment and Reviews

The information security team constantly seek out and assess potential security risks and work to eliminate or minimise those risks to an acceptable level. Any risk deemed of a nature that could cause a significant issue to a client, individual or the Business would be immediately escalated to the COO and IT Director whereupon a resolution would be determined and actioned. The list of risks is maintained in a register and whilst constantly reviewed, there is at least one formal annual review with outcomes reported to COO.

Physical Security

We undertake reasonable steps at all times to protect our IT infrastructure from unauthorised access. Any NHS servers are held in secure ISO27001 compliant data centres which have numerous safeguards such as 24/7 security, government ID required, escorted personnel only, bio-metric sensors in addition to protection from environmental impacts. On-site networking equipment is kept in locked racks in locked rooms with access granted to only those that need it. When not in use, all laptops are locked in cupboards. Access to floors is via electronic door passes and/or PIN code locks. A clean desk policy is in force.

Network Security

Firewalls and web filtering act as a level of protection on our network. All access to our networks requires authentication and Wi-Fi connections are encrypted. Access to our data centre is done over a secure VPN. Access logs and login attempts are monitored. Our networks are constantly scanned for vulnerabilities and remediating action taken as soon as possible. Independent pen-testing is conducted at least annually.

Endpoint Security

All laptops and desktops have full disk encryption and require users to authenticate with a passcode before access to the device is granted. The endpoints run anti-malware software, the status of which is centrally monitored. The operating system and software are regularly patched and updated, and all machines undergo at least weekly additional vulnerability scanning. All users run as standard (non-admin) user rights. Each device has a number of configuration and compliance policies that are monitored centrally and any machine that for whatever reason becomes non-compliant can no longer access core services. Similar policies are applicable to the use of mobile phones for business use. All IT equipment is disposed on securely at the end of its life.

Data Confidentiality

In day-to-day business, The Groves Medical Group does not undertake the processing of personally identifiable data other than that of its employees in a normal HR and payroll capacity. All client data is treated as confidential and appropriate safeguards are in place to store and transfer it safely. During transit, data would be encrypted. Access to data is given on a needs-only basis and removed as soon as possible. Data will only be used for the purpose it was intended and will be destroyed when no longer needed.

Emails

All emails passing through our server are scanned for malware. Inbound and outbound spam protection is also in place. With the rise and complexity of phishing attempts seen as a continuing threat, The Groves Medical Group undertakes regular end-user education as well at monitoring and blocking known-bad links.

Passwords and Access

All our systems are covered by complex passwords that require being changed on a regular basis. On our core systems and those that store client data, additional two-factor authentication is in place. Passwords are not shared, and education is provided about the storage and use of passwords.

Further information can be found in our Access Control Policy.

Data Transfer

As part of any project with a client that involves us processing their data, details of how data will be securely transferred will be discussed with The Groves Medical Group ’s Information Security team to ensure a robust and secure process is in place to manage transfers. This would normally involve only allowing data to be transferred over a secure connection, use of encrypted data files, logs maintained, and data deleted as soon as no longer required. Data will only be made available to those working on specific projects.

Operating Systems and Software

In order to maintain secure platforms, The Groves Medical Group strives to patch operating systems and software as soon as any known vulnerabilities become known about. Vulnerability scanners constantly monitor endpoints, servers and networks to identify issues and The Groves Medical Group aim to patch anything deemed high risks as soon as possible (usually under a week).

Education

Whilst technology can go a long way to monitor and prevent some cyber-risks, users very often can be a weakness. As a result, The Groves Medical Group undertakes mandatory regular training for all staff in information security and provide regular reminders, seminars and best-practice advice on how to reduce The Groves Medical Group's exposure to cyber-risks, as well as making sure all staff are clear on their responsibilities and the processes to report any incidents or concerns.

Resilience

In order to ensure that business can continue in the event of unforeseen circumstances, The Groves Medical Group have a number of measures in place to ensure business continuity. From a cyber-perspective, this includes the availability of redundant resources, including networking equipment, data lines and hardware.

Backups are taken daily and stored in secure separate-site locations.

Full details are covered in our Business Continuity Policy and Plans.

Disciplinary Action

The Groves Medical Group take infringements of our Information Security Policy (of which this is part) extremely seriously, and all staff are aware of the consequences of actions that could expose data or increase likelihoods of attack. In such cases, there is a procedure in place that would result in disciplinary action. That action would be commensurate with the nature of the infringement and the intent.