Acceptable Use Policy

[July 2022]

Contents

Policy Owner	IT Director
Date of last review	March 2022
Date of next review	January 2023
Changes Made:	First Draft for approval at ExCo
Changes Made:	Updated from ExCo
Changes Made:	
Current Version	V1.1

NAME	: Sam Duncan
SIGNED AS	: Sam Duncan
SIGNATURE	: Sam Duncan Sam Duncan (Apr 14, 2023 13:44 GMT+2)
EMAIL	: sduncan@openboxsoftware.com
DATE	: 14/04/23

1. Purpose

Protecting our business is a responsibility we all share and requires the right balance in giving our people the freedom to succeed whilst enforcing guidelines and policies that ensure that we work safely, securely and responsibly.

This policy sets out how we manage and handle our IT equipment and data, and the standards that must be observed when using and/or accessing them.

The misuse of Grainger PLC's IT equipment and data can seriously damage Grainger PLC's business and reputation, and therefore it is extremely important that all staff, including employees, contractors and relevant third parties, read and understand the policy – as the responsibilities outlined must be followed in full.

Breaches of this policy may be dealt with under the Disciplinary Process in the Employee Handbook and, in serious cases, could be treated as gross misconduct leading to summary dismissal.

2. Introduction to the Policy

Grainger PLC's data is essential to the current and future success of the business. Maintaining the security and availability of Grainger PLC's data is a necessity and is core to our business.

We are required to ensure that Grainger PLC data is not at risk through loss or unauthorised modification (whether deliberate or inadvertent) and that the integrity of our data is maintained throughout its lifecycle.

Grainger PLC has legal, statutory, regulatory and contractual obligations that include information security. Furthermore, we need to demonstrate information security to our customers. Grainger PLC's information security policies, standards and procedures assist us in achieving these goals. You have an obligation to adhere to these policies, standards and procedures.

Information security is the preservation of the confidentiality, integrity and availability of information:

- Confidentiality – Protecting sensitive or personal information from unauthorised disclosure, both to outsiders, and to employees or contractors who have no requirement to access such information in the course of their duties.
- Integrity – Safeguarding the accuracy and completeness of information and information processing methods, against any unauthorised changes.
- Availability – Ensuring that information and associated services are available to meet Grainger PLC's business needs.

Information security is required during the whole lifecycle of information based in Grainger PLC, from the moment it is collected or created, throughout its usage, to ultimate disposal. Appropriate measures need to be applied to ensure that information security is maintained. Information security promotes trust and confidence in Grainger PLC's services, business practices and IT infrastructure and systems.

The achievement of information security requires a combination of policies, standards, procedures, appropriate organisational structure, physical security considerations, and measures to safeguard the IT network infrastructure and information systems.

If you need assistance on any of the information security requirements contained in this policy, you should seek advice from your line manager or from the Security and Configuration Manager.

3. Scope

This policy applies to all Grainger PLC staff irrespective of status, including temporary staff, contractors, consultants and third parties who have access to Grainger PLC's data and systems.

It applies to the use of all facilities, equipment and systems that process or store Grainger PLC's information.

It applies whether the access to and use of systems and data occurs on Grainger PLC's premises or remotely from any location including, but not limited to, home working.

4. Policy Statement

Grainger PLC's policy is that our facilities, equipment, systems and data shall only be used and accessed in acceptable ways that ensure the confidentiality, integrity and availability of the information.

5. Roles and Responsibilities

- The Executive Committee shall ensure the Grainger PLC continuous security improvement programme is aligned to business objectives, communicate the importance of effective information security management and conforming to policy requirements and provide the programme with sufficient resource to succeed.
- The Information Security Forum (ISF) is responsible for this policy and shall ensure that this policy is up-to-date and relevant. The ISF are responsible for ensuring the Executive Committee are informed of progress and relevant issues/risks.
- The Chief Information Officer (CIO) is accountable for the continuous security improvement programme at Grainger PLC.
- The IT Director has responsibility for the day-to-day operation of the continuous security improvement programme and for monitoring its performance, reporting to the CIO and ISF. The IT Director is supported by a Security & Configuration Manager.

- Line managers are responsible for ensuring that their staff comply with this policy. All authorised users shall adhere to this policy. Non-compliance shall be subject to investigation and may result in disciplinary action.

6. What Is Your Responsibility?

You are personally accountable for assisting Grainger PLC in maintaining the confidentiality, integrity and availability of its information.

All staff are faced with information security risks and responsibilities daily. Effective security management is about mitigating our risks. From an organisational perspective, this has been achieved through the development of information security policies, standards and procedures, together with complementary information security training and awareness.

Poor information security management can, for example, lead to:

- Leakage and compromise of sensitive information, eg personal or commercial information.
- Loss of critical information.
- Fraudulent activities, eg identity theft; and
- Failure to comply with legal, statutory, regulatory or contractual requirements.

A direct result of such an occurrence could be that our business, research opportunities and relationships with our customers will suffer. In order to avoid such instances, we shall all take necessary steps to ensure that security is maintained, including the following:

- Ensure that Grainger PLC's Information Security Policy requirements are complied with at all times.
- Obtain advice from line managers, or the IT Team when unsure.
- Request training when needed.
- Complete training when required.
- Report any suspected security incidents to the IT Service Desk; and
- Make recommendations on how we can improve our information security.

Enabling Grainger PLC to operate in a secure environment requires us all to work as a team towards the same goal of information security.

7. Acceptable Use of IT Assets

All IT processing facilities and equipment to be used in connection with Grainger PLC's information shall be formally configured and authorised by the IT Department and approved by relevant asset owners or line managers before such use. Staff are not permitted to use personally owned devices for any Grainger PLC business.

The IT Department shall use and maintain a documented list of approved products, used for selecting IT equipment, and shall manage an inventory of all acquired IT assets. This includes recording of personnel authorised to use the IT assets, and any labelling requirements for the IT assets. All IT assets shall be returned to the IT Department when they are no longer required – this will help maintain the IT asset inventory.

All of the IT equipment, devices and software that you have been assigned remains the property of Grainger PLC. You have an obligation to ensure that this equipment and software is safeguarded and only used as intended by Grainger PLC:

- You shall always take care of IT equipment allocated for your use and treat it as if it is your own.
- You shall protect your IT equipment against theft and unauthorised access.
- You shall not store any access control device with equipment or devices which are reliant on the same device for multi-factor authentication.
- You shall not expose your IT equipment to any environmental hazard, such as extremes of temperature.
- You shall not install any unauthorised or unlicensed software on your IT equipment. If you require any software for your work, you shall get approval from your line manager and the Service Desk.
- You shall not modify your IT equipment in any way; this includes any amendments to the hardware and software configuration.
- You shall not install any unauthorised tunnelling (VPN) or peer-to-peer software or service.
- You shall not install any monitoring avoidance software or service.
- You shall always report any IT problems to the Service Desk as soon as possible.
- Equipment is provided for sole use by the Grainger Employee.
- When returning equipment you shall ensure it is in an acceptable condition. Grainger PLC reserve the right to charge for any damage to IT equipment.

Specific acceptable use requirements in connection with protection against malicious code such as viruses and spyware, secure use of e-mail and Internet access, and protection of copyright materials are documented below.

Grainger PLC provides primary access to its systems and IT equipment for business use, but recognises that there are times when you will need to complete personal tasks online, and reasonable personal use of equipment is permitted.

When you use Grainger PLC equipment assigned to you for personal and/or business matters, you shall ensure that you do not:

- Violate any laws, professional standards or Grainger PLC policies.
- Create the appearance of impropriety on the part of Grainger PLC.
- Violate or infringe upon the intellectual property rights and property of others.
- Put the rights and property of Grainger PLC or its customers at risk.
- Compromise, embarrass or bring into disrepute Grainger PLC's brand, reputation or relationships with its clients.
- Utilise Grainger PLC identities, including business e-mail address(es), for personal accounts or services.
- Impede any Grainger PLC business activity, including your own productivity.
- Impersonate others or position yourself as an authorised spokesperson for Grainger PLC in online forums or social media without prior written approval, in line with the Grainger PLC Social Media Policy.

If you are using Grainger PLC equipment for personal use (such as conducting online banking, booking a holiday or shopping) you do so at your own risk, and, if you have any concerns about the security of Grainger PLC's equipment, you shall use alternative means for conducting your personal business. Employee Wi-Fi access is provided such that you can use your own device for personal use. (A Wi-Fi guest network may also be available for visitors).

8. Site Security

Physical security involves protecting Grainger PLC's premises, staff, information and IT assets from unauthorised physical access and physical security threats, e.g. fire, invasion, theft and wilful damage. All staff shall support Grainger PLC's site security requirements. Staff shall not allow unauthorised physical access into Grainger PLC's offices, computer rooms and sensitive areas, and shall report physical security threats to Office Managers as soon as possible using Grainger PLC's standard reporting procedures.

If you are allocated with keys or other controls (such as swipe cards) for access to Grainger PLC's offices or facilities, ensure you keep them in a secure location, and protected from unauthorised access. If they are lost or stolen, you shall immediately report this to Office Managers, in line with the Incident Management Policy and Personal Data Breach Notification Procedure.

Do not allow anyone to 'tailgate' when you are entering a perimeter door of a building or a secure area. If you are suspicious of any individual, tactfully challenge them to ensure that they have a legitimate reason to be there, and have authorised access. Unauthorised personnel shall not be permitted to enter a building or a secure area and shall never be unescorted.

Visitors, for whom you are responsible, shall always report to reception, identify themselves and be escorted within Grainger PLC's offices at all times (unless otherwise authorised).

More information can be obtained from the Physical Security Policy.

9. Removal of Property and Security of Equipment Off-Premises

Other than laptops and mobile devices assigned to staff for their permanent use, Grainger PLC’s IT equipment shall only be taken off-site following formal authorisation by the IT Department, whilst Grainger PLC’s information shall only be taken off-site following formal authorisation from the relevant asset owner or line manager.

All staff are responsible for protecting authorised off-site equipment (allocated to them) against physical security threats and unauthorised access. See section 19below for more detail.

10. Secure Disposal and Re-use of Equipment

All of Grainger PLC’s information and software shall be securely wiped from Grainger PLC’s IT equipment before disposal or re-use of the equipment. All equipment intended for disposal and re-use shall be returned to the IT Department, who shall securely wipe Grainger PLC’s information and software from it, using established procedures.

Where data cannot be securely wiped the media shall be removed or securely destroyed to ensure the information cannot be later retrieved.

11. Protection against Malware

Computer viruses, spyware, remote access Trojans, ransomware and other forms of malicious code (malware) exploit vulnerabilities in software programs and can cause loss and damage to Grainger PLC’s information, software and IT equipment or unauthorised access to Grainger PLC systems and services.

Grainger PLC uses a variety of products, eg monitoring, anti-virus and software security patches, to reduce the threat from viruses and other malicious code. You shall not change or remove these controls on your Grainger PLC PC or laptop, otherwise Grainger PLC’s IT network, systems and information will become more vulnerable to the threat from viruses and other malicious code.

In addition to these controls, Grainger PLC is also dependent on its staff, who shall remain vigilant to protect Grainger PLC from malicious code. You shall ensure that:

- You do not introduce a virus or malicious code into the corporate network, by downloading unauthorised or suspect software from the Internet or from computer media, eg USB storage or smart devices onto your PC, laptop or any Grainger PLC system or service.
- All software and data which originates from outside Grainger PLC shall be checked for viruses and malicious software prior to it being opened or used – if you need help, contact the Service Desk.

- If you are suspicious of a virus or malicious code, you shall stop using your PC or laptop immediately and contact the Service Desk.
- If you receive a suspicious e-mail, you shall not open or preview it, or the attachment or any hypertext link, as this may well activate a virus or other form of malicious code. Immediately contact the Service Desk. Grainger PLC have configured your email account to ensure all external emails are highlighted with a banner titled 'CAUTION: External Email'.

There may also be 'hoax' virus messages in circulation which are not actually viruses at all, but plain e-mail messages asking you to take some sort of action, such as deleting files on your computer and forwarding the message which then due to the number sent become 'viral' themselves. These messages themselves are not infected with a virus, and are spread by playing on people's fears, and fooling them into following the instructions. If you receive a message warning you of a virus, you shall immediately contact the Service Desk.

More information can be obtained from the Malware Protection Policy.

12. Secure Handling of Media and Documentation

Care shall be taken to protect all documentation and computer media, e.g. smart devices containing sensitive and critical information, and measures shall be taken to ensure secure storage, transit, copying, reuse and disposal of computer media and documentation.

When exchanging information within Grainger PLC or between Grainger PLC and other organisations, it is vital to assess the sensitivity of the information.

The use of USB devices poses a risk to Grainger PLC in respect of loss of data and other intellectual property, and potential introduction of malware. As such, the use of USB devices are not permitted by default.

When dealing with printed documents, always ensures that you are aware of their security classification and handling requirements. Sensitive documents shall not be left or reviewed in public or on public transport, or left unattended on desks, printers, facsimiles and other equipment where they are vulnerable to unauthorised access and theft. You shall always lock sensitive computer media and documents away when left unattended.

13. Storage of Information in the Cloud

Users shall only store or share Grainger PLC information in the Cloud using products and services approved by Grainger PLC which includes SharePoint and OneDrive. The IT Department shall be consulted before any attempt to store information with a Cloud Service Provider that is not approved by Grainger PLC.

Staff must be aware that some financial and personal Grainger PLC information may be subject to legislation, including but not limited to data protection legislation, where cloud services used must restrict the storage of Grainger PLC or other information to a particular geographic region.

You must gather authorisation from the applicable Asset Owner before utilising data transfer mechanisms, such as third party instances of Microsoft Teams. The Asset Owner must ensure the third party systems are legitimate and secured. Contact the Service Desk for more information or clarification.

14. E-mail Security and Secure Internet Access

E-mail, Internet and communication tools such as Microsoft Teams are provided to you as a means of improving your communications, collaboration, knowledge and effectiveness at work. Communication tools are intended for business use. All usage of Grainger PLC’s e-mail and Internet facilities is treated as the property of Grainger PLC and shall not be regarded as private.

Grainger PLC e-mail or other communication tools may not be used for exchange of inappropriate (including pornographic, obscene, offensive, racist, defamatory, harassing or intimidating) content, to facilitate personal financial gain, or for political purposes.

Staff shall be aware that Grainger PLC reserves the right to use monitoring tools to enforce Grainger PLC policies, retain information from and about e-mails/messages exchanged, and will produce periodic reports detailing use of all e-mail and Internet access facilities.

Use of e-mail, communication tools and Internet access introduces security threats such as malicious code attacks, eg viruses, unsolicited or undesirable e-mails, attempt to initiate financial transactions, fraudulent attempts to acquire sensitive information such as passwords. If you accidentally access any material which is not permitted, you shall report this to your line manager and the Service Desk immediately.

E-mail is an insecure method of communication and messages may well be read by those who have no authority to do so. Before sending information via e-mail, you shall first assess the handling requirements of that information as established and if e-mail is the correct means to exchange data. Encryption guidance is available from the IT Department.

Grainger PLC e-mail may not be auto-forwarded to a third party or public e-mail system unless there is an approved documented business need.

15. Information Security in Conversations and with the Use of Telephones and Recording Equipment

Due care shall be taken when using telephones, voicemail, conferencing, answering machines and recording equipment (eg photographic, video and audio equipment) to ensure the protection of sensitive information. Staff shall comply with the Data Protection Policy.

It is important that before you conduct a telephone conversation in an open plan office area or outside of Grainger PLC's premises, you shall consider the nature of the topic you are about to discuss. If the conversation is of a sensitive nature, you shall ensure that there is no possibility of eavesdropping. Remember to always be aware of who is around you when holding a confidential conversation. In addition, messages containing sensitive Grainger PLC information shall not be left on voicemail and answering machines.

16. User Identification, Access and Monitoring

You shall only access and use Grainger PLC's IT network, systems and applications if you are authorised to do so. If you are granted access, it is so that you are able to perform your duties efficiently.

You shall remember that access has been granted for your sole use by means of a unique user account and password. This applies to the different user accounts that may be granted to you for access to Grainger PLC's network, information systems and applications. You shall not give details of your user account and password to anyone, including your line manager; you shall not share any user account allocated to you with anyone else. Grainger PLC (within its legal rights) is able to track the activities of each user via their user account, and identify exactly what information and systems or services they have accessed and what actions have been taken. If it is your user account that is logged as attempting an unauthorised or illegal action, you may be held responsible. It is in your interests to ensure that you safeguard your user account and password details at all times.

In order the ensure compliance with legislation, regulations, contracts and its information security policies, Grainger PLC reserves the right to monitor user activities and data flows.

17. Password Security

Passwords are a key control to maintain information security. They help us ensure that only authorised persons have access to Grainger PLC's IT network and systems. In order for your password to be effective and remain secure, you shall comply with the following simple rules.

Passwords shall be kept confidential at all times and shall not be disclosed to or shared with anyone, not even your line manager or the IT Department. Shall someone require approved access to your information (eg long term absence) it can be shared through other means. Contact the Service Desk for more information.

Ensure that your password is memorable, so that you do not need to write it down or electronically store it. Written down passwords are strongly discouraged. Electronically stored passwords are strongly discouraged, unless the passwords are secured via an IT solution that is approved by the IT Department and the Security and Configuration Manager. Online text or documents for passwords shall never be used.

Ensure that your password is difficult for others to guess. When creating your password, you shall always use good password practice:

Password Settings	Complexity Rules
Complexity	• 8 characters in length • Uppercase characters (A through Z) • Lowercase characters (a through z) • Numbers (0 through 9) • Special characters (for example: !, $, #, %).
Changes	Passwords shall be changed at least every 90 days.
History	The last 12 passwords shall not be re-used.

- DON'T (individually or as a combination of):
  - Use your user ID.
  - Use names (eg your name, or the names of your partner, children and heroes, or place names).
  - Use information which is well known to others, or could be gleamed through social media (e.g.: hobbies, brands, holiday resort destinations, family/pet names, celebrities).
  - Use dates (eg birthdays, anniversaries, other memorable, recurring or dates associated with significant/major events).

- Use words that people can associate you with (eg birthplace, home address, Grainger PLC's address, sporting team(s)).
- Use words from any dictionary (e.g.: local and any second languages you may use).
- Use the same password for all different applications and platform – if one becomes breached they all are.
- Use the same password between business systems and personal accounts – if one becomes breached they all are.
- Use successive passwords that follow an easily predictable pattern (e.g.: [Password]01, [Password]02, [Password]A, [Password]B).

Ensure that you are not overlooked when typing your password. If your password is disclosed to anyone or compromised in any way, you shall change your password immediately. Always contact the Service Desk to discuss any issues regarding your password.

18. Clear Desk and Clear Screen

Measures shall be taken to adequately protect against unauthorised physical access to Grainger PLC's information hosted on PCs, laptops, handheld devices (eg tablets, mobile telephones, and digital cameras), computer media (eg DVDs, CDs and USB storage devices), and paper documentation.

All staff shall ensure that access to their user accounts is password protected when their computer devices are left unattended, even for a small amount of time, eg 1 minute. This can be done by following these simple steps:

- Press Ctrl, Alt, Delete buttons together.
- A dialog box will appear. Within this, click on the 'Lock This Computer' option.
- Alternatively, press the 'Windows' button and 'L'.

All staff shall ensure that all mobile equipment, eg laptops and tablets, sensitive computer media and sensitive documentation are not left unattended and insecure, but are appropriately stored in locked areas or facilities, eg locked cabinets, and that access to relevant keys is controlled.

At the end of a working day, you shall:

- Logoff from and shut down your PC or laptop.
- Clear your desk and lock all sensitive computer media and documents away in a drawer or cabinet with suitably restricted access.
- If you are a user of a laptop or handheld device, and you are not taking it with you, you shall lock it away in a drawer or cabinet with suitably restricted access.

19. Remote Working

Remote workers include:

- Mobile workers: all users who use Grainger PLC's information and information processing facilities whilst not located on Grainger PLC's premises, eg workers who are located in other organisations' offices, in hotels and conferences, and travelling workers.
- Home workers: users who have been authorised to use Grainger PLC's information and information processing facilities whilst based at home, or larger groups of Grainger PLC employees required to work from home during exceptional periods of disruption or mandatory changes to working practices.

Laptops, mobile phones, tablets, and other such portable equipment are expensive and valuable assets that are highly desirable, particularly to the opportunist thief. Loss of such equipment not only has an obvious financial implication, but may also compromise the information that is on the equipment itself. Exposure of this information could result in breaches of Grainger PLC's legal, regulatory, statutory and contractual obligations, and damage to Grainger PLC's reputation. For example, the loss of a laptop which holds a file containing personal details of employees is likely to result in contravention of data protection legislation. This could lead to Grainger PLC, and possibly the individual concerned, facing a fine or in extreme circumstances imprisonment.

Users shall check the name of the wireless network they are connecting to, to determine whether it appears to be genuine. Users shall use the Grainger supplied VPN (Citrix Netscaler) at all times when using public Wi-Fi. If in doubt, users shall not connect to the network. Unsecured networks should not be used, and tethering of Grainger supplied mobile devices should be used if required.

International remote working is possible when there is a business need, subject to prior agreement with Executive Committee Managers and IT. Users must inform IT before traveling as high-risk countries are routinely blocked through geo-fencing to prevent malicious activity.

20. Reporting Information Security Incidents

In order for Grainger PLC to be able to manage and deal with information security incidents successfully, they shall be captured and logged.

If you suspect or have knowledge of an information security incident or event, or a breach of Grainger PLC's information security policies or procedures, or a software malfunction, or a security weakness in any Grainger PLC building, network or information system, you shall report the concern immediately in accordance with the Incident Management Policy.

Examples of an information security incident include:

- Compromise of personal or sensitive information, eg commercial data or personal data.
- Malware being discovered on one or more devices.
- Physical damage to Grainger PLC equipment that stores, retrieves, transmits or manipulates information.

- Events that significantly disrupt the availability of Grainger PLC resources.
- Unauthorised use of another user's profile (masquerading of user identity).
- Divulging a password to another user without authority.
- Improper use of email or the Internet, eg downloading or distribution of unauthorised software, and non-business related activities that rise above acceptable use.
- Unauthorised copying and/or distribution of Grainger PLC information.
- Damaging or impairing the functioning of Grainger PLC resources in a manner that may impact information security.
- Unauthorised access to Grainger PLC resources from internal or external sources.
- Theft of Grainger PLC resources.

Remember, it is vital that you report all confirmed or suspected information security incidents. Withholding information or failing to report an incident could result in you being held personally liable. Staff shall not attempt to deal with the information security incident (other than reporting the incident), otherwise they may become involved in disciplinary or legal action. Incidents must be reported via the IT Service Desk application or by telephone (0191 269 5989).

If in doubt, please contact the Security & Configuration Manager, IT Director or your line manager for advice.

21. Intellectual Property Rights (IPR) and Copyright Legislation

All staff shall observe intellectual property rights and copyright legislation. The main purpose of such legislation is to protect the developer of the information, software, or other original material, and prevent its improper use. If it is necessary to make copies of such materials, the express permission of the copyright owner shall be granted first. In addition, a user licence is normally required to use copyrighted software.

Only authorised, legal software shall be stored and processed on Grainger PLC's IT network and systems. You shall not install or copy any software on Grainger PLC's IT equipment, eg music files. If you require any software for your work, you shall firstly consult your line manager and the Service Desk.

Software developed by staff whilst working for Grainger PLC is the intellectual property of Grainger PLC, and it shall not be used for any other purpose outside of Grainger PLC's authorised business requirements.

Users shall not copy and distribute hardcopy documentation that is copyright protected without authorisation by relevant Grainger PLC information owners and line managers.

22. Data Protection Legislation and Privacy of Personal Information

Data protection regulations, including the General Data Protection Regulation (GDPR), are concerned with the direct use of personal information, whether that information is a manual record or processed on a computer system. Data protection legislation and regulations apply to all types of personal information; this includes information which may not be thought to be confidential.

Personal data means data that relates to a living individual who can be identified from that data, or a combination of that data and other information which is in the possession of Grainger PLC. It also includes any expression of opinion about the individual.

The GDPR has data handling principles, all of which shall be adhered to when handling personal information. The principles include specific requirements that address the security aspects of handling personal information.

If Grainger PLC fails to abide by data protection legislation and regulations, it could be heavily fined and its business operations could be negatively impacted. Personal liability is also imposed, so if an employee is found to be contravening data protection requirements, he/she could be prosecuted too.

All staff shall comply with data protection legislation and regulations, and the Data Protection Policy.

23. Computer Misuse Legislation

All users shall comply with applicable computer misuse legislation. Such legislation, generally aimed at computer ‘hacking’, specifies offences for any unauthorised access to internal organisational systems.

Computer misuse legislation generally defines as criminal acts:

- Unauthorised access.
- Unauthorised access with intent to commit a further serious offence.
- Unauthorised modification of computer material.

Staff shall only access systems they are authorised to use. It is an offence to knowingly gain unauthorised access to a computer system, and this could result in a fine or imprisonment.

24. Policy Review Date

This policy shall be reviewed and appropriately updated on an annual basis. It shall also be reviewed and appropriately updated when there are any changes to relevant regulations on information security and/or data protection.

Signature: N Papenfus
N Papenfus (Apr 14, 2023 14:16 GMT+2)

Email: npapenfus@openboxsoftware.com

Signature: Genevieve Godlonton
Genevieve Godlonton (Apr 17, 2023 10:31 GMT+1)

Email: ggodlonton@openboxsoftware.com