

Data and IT Security Procedure and Policy

Introduction

This document describes the requirements, controls, security measures, responsibilities and processes that are necessary to safeguard Magicman (The Company) data and information technology infrastructure and systems (IT Systems).

Conditions of Use

By accessing or using The Company's IT Systems and data, employees are bound by the conditions outlined in this document.

Employees and users are not permitted to attach personally owned devices to IT Systems equipment or networks.

These Conditions of Use apply to all users of IT Systems, including but not limited to, all members of employees, temporary users and any visitors.

Definitions

For the purposes of these Conditions of Use, IT Systems are defined as:

- email
- the Internet, intranet, and any other networks
- all desk top computers
- laptops
- other mobile devices
- any other related software and hardware.

IT Systems also includes any property of The Company purchased, leased, rented or on loan from third parties. This also includes any software or other applications licensed to or used by The Company.

For the purposes of this procedure Data may include:

- Information that is held or transmitted verbally, electronically or in hardcopy
- Database content
- Reports
- Meeting minutes
- Inspections and audit findings
- Personal details and records
- Commercial information
- Financial information
- Contractual information
- Visual information

Employee Requirements

1. Employees shall not carry out any action, including loading any software onto IT Systems, that:
 - may interfere with the normal working of IT Systems
 - may interfere with or disrupt other users' use of IT Systems
 - accesses, corrupts or modifies any other user's data without their consent.
2. Employees shall not deliberately introduce a virus, worm, Trojan Horse, SpyWare, or other similar code. Nor shall they take any action to circumvent or reduce the effectiveness of, any anti-virus or other malicious software detection, removal and protection precautions.
3. Employees are solely responsible for the use of your username. They shall not make their username or password available to anyone else nor shall they use any other person's username.
4. Employees shall not install or play games on IT Systems.

Prepared By	Reviewed By	Approved By	Version 1
Susie Wall	Poppy Henderson	Mark Henderson	August 2024

5. Employees shall not tamper with the configuration of any IT Systems, including any cables or peripheral devices attached to IT Systems.
6. Employees shall not use any sort of device (e.g. memory stick, flash drive, etc.) with IT Systems without the prior approval of the IT Manager.
6. Employees shall not use IT Systems in any way that could expose them or The Company to any criminal or civil liability. For example, employees:
 - a. Software – shall only use software in accordance with the terms of the relevant licence. Copying software without the licence holder's permission is prohibited.
 - b. Rights in content – shall not use third-party text, images, sounds, trademarks, and logos in materials such as emails, documents, and web pages without the consent of the rights holder.
 - c. Offensive material – shall not use IT Systems or websites to access, store or distribute material that is obscene, indecent, malicious, or pornographic. If the Company suspects that someone has accessed or used material that might give rise to criminal liability, it may notify the police.
 - d. Discrimination and harassment – shall not create, distribute or access material that is: gossip about colleagues or management, for personal gain, unlawfully discriminatory, including on the grounds of age, sex, sexual orientation, race, disability or religion, that might incite any form of violence or hatred, or to cause harassment, alarm or distress.
 - e. Computer misuse – shall not gain unauthorised access to accounts (including stealing or misusing a password), programs and/or data. All forms of hacking are prohibited and may be an offence under the Computer Misuse Act 1990 (see Section 5.1).
 - f. Defamation – shall avoid content which may be defamatory. Care is needed when sending material electronically or by posting material on the Internet (e.g., through web pages and or social media).
 - g. Data – must access, store, process and back-up data owned, processed or held by The Company, in a manner appropriate to its security classification. Failure to appropriately classify and handle data is a breach of these Conditions of Use.
 - h. Personal data - who hold personal data, with few exceptions, must do so in accordance with the principles set out in the Data Protection Act 2018 (see Section 5.2), which implements the European Union's General Data Protection Regulation (GDPR).
 - i. Formation of contracts – shall take care when forming of contracts electronically, without any hard copy confirmation from the user, i.e. care should be taken to obtain appropriate authority before purporting to commit The Company to any contractual obligations, which may include clicking 'I agree' to an online dialogue box. The wording 'subject to contract' should be used on emails where appropriate.
 - j. Unsolicited and offensive e-mail – are prohibited from sending unsolicited e-mail or other mass e-mails (spam) to single or multiple recipients. This includes forwarding advertisements or replying inappropriately to an entire mailing list. Employees shall not send email that any employees member that may reasonably cause offensive or likely to cause annoyance or needless anxiety, in particular any that would be in breach of sub-paragraphs (c), (d) and (f) above.
 - k. Email/data received in error - when receiving an e-mail message (not SPAM) which has been wrongly delivered to your e-mail address, should notify the sender of the message by immediately redirecting the message to that person. Furthermore, in the event the e-mail message contains confidential information, you must not disclose or use that confidential information. Should you receive an e-mail which contravenes this policy the e-mail should be brought to the attention of IT Manager and HR Manager.
 - l. Social network/media sites – shall not access any social network/media sites with reference to Magicman or its employees, clients or suppliers without permission or instruction from senior management. In addition, they shall not post information on such sites which is or may be confidential or detrimental to The Company, its suppliers, customers, or other employees.

Monitoring and Privacy

The Company acts in accordance with applicable legislation and the Information Commissioner’s Employment Practices Code, notably in relation to the monitoring of communications.

The Company undertakes some routine monitoring of activity on IT Systems to ensure that they operate correctly and to protect against the risk of harm from viruses, malicious attack, and other known threats. This does not normally involve the monitoring of individual communications (but can do) or the disclosure of the contents of any user files.

Prepared By	Reviewed By	Approved By	Version 1
Susie Wall	Poppy Henderson	Mark Henderson	August 2024

The Company reserves the right to monitor all use of IT Systems, including company phone use, emails sent and received, and web pages and other online content accessed:

- a) to assist in the investigation of breaches of these Conditions of Use.
- b) to prevent or detect crime or other unauthorised use of IT Systems.
- c) when legally required to do so, for example as part of a police investigation or by order of a court of law.

Where such monitoring is necessary in pursuit of other business interests, for example to review the emails of employees on long-term sick leave or to disclose documents under the Freedom of Information Act 2000, it shall only be carried out if prior authorised by The Company's CEO. IT Systems users should therefore assume documents such as emails could become known to others.

IT Systems are available principally for employees to carry out their work. However, The Company realises that occasionally employees will use IT Systems for your own personal purposes. They can make personal use of IT Systems only if such use:

- a) does not interfere with the performance of their work.
- b) does not incur unwarranted expense on The Company.
- c) does not have a negative impact on The Company or bring it into disrepute (i.e. that may be derogatory, defamatory, discriminatory, or offensive).
- d) does not involve downloading music or other internet content;
- e) does not involve creating a non-work-related website.
- f) does not involve the unauthorised downloading software; and
- g) is otherwise in accordance with these Conditions of Use.

If you publish information on the internet using the IT Systems additional regulations apply.

If employees use of IT Systems is in breach of these Conditions of Use, The Company may take disciplinary action.

Allegations

Where an allegation has been made against a member of employees, The Company has the right to inspect, review and take copies of any material held in the name of that employee on any device that might provide evidence for or against the allegation.

Breaches

Where an alleged breach of these Conditions of Use is brought to the attention of the CEO, all reasonable measures will be taken to investigate whether the allegation is justified. Following such an investigation, necessary steps may be taken to prevent further breaches. This may involve inspecting the contents of a user's files or email messages. However, inspection and copying of a user's files shall only be undertaken if authorised by the CEO.

If a complaint or allegation is made against a user, their access may be immediately suspended for investigation. Disciplinary penalties for breach of these Conditions of Use can include dismissal. The Company may refer the user to the police where appropriate and it will co-operate fully with any police investigation.

Day-to-Day Working Practices

- a. The Company has IT security systems in place but cannot guarantee that these will prevent every attempt to access confidential or restricted data. Employees shall ensure that confidential material is password-protected and/or encrypted as appropriate to prevent unauthorised access by third parties.
- b. If employees do make use of IT Systems for personal use, they should be aware that it may be possible for personal information to be inadvertently accessed during enforcement of these Conditions of Use.

Prepared By	Reviewed By	Approved By	Version 1
Susie Wall	Poppy Henderson	Mark Henderson	August 2024

Security Management

The Company must protect data using all means necessary including the prevention of security incidents. A computer security incident may involve:

- a) loss of confidentiality of information
- b) compromise of integrity of information
- c) denial of service
- d) unauthorised access to systems
- e) misuse of systems or information
- f) theft and damage to systems
- g) virus attacks
- h) intrusion by humans

Other incidents that put data and IT security at risk include:

- a) Loss of ID badge/s
- b) Missing correspondence
- c) Exposure of Uncollected printouts
- d) Misplaced or missing media
- e) Inadvertently relaying passwords
- f) Loss of mobile phones and portable devices

Security-Related Working Practices and Techniques

All employees are required to apply diligence when working for The Company, particularly where security of the business is paramount. Failure to observe sensible working practices can result in security incidents. The following guidelines should be followed:

Computers left unlocked when unattended

Users of IT Systems are reminded of the importance of locking their computers when not in use or when leaving computers unattended for any length of time. All employees need to ensure they lock their computers - this must be done even though The Company’s computers are configured to automatically lock after 15 minutes of idle time.

Password Security and Disclosures

Unique IDs and account passwords are used to allow an individual access to systems and data. It is imperative that individual passwords are not disclosed to others – regardless of trust. If an individual needs access to data or a system, they must go through the correct procedures for authorisation – initially through the individual’s Line Manager. If anyone suspects that their or any other user’s password has been disclosed whether intentionally, inadvertently, or accidentally, your Line Manager must be notified immediately.

Password Rationale: Passwords are used with the aim of protecting the confidentiality, integrity and availability of data held by The Company. Passwords should be sufficiently strong (e.g. long and complex) as to thwart brute-force attempts at guessing them.

Password Length: All Company passwords shall be a minimum of eight characters long. This is in line with industry best practice.

Password Complexity: Company passwords shall contain characters from at least three of the following categories:

- i. English uppercase characters (A-Z)
- ii. English lowercase characters (a-z)
- iii. Digits 0 to 9
- iv. Non-alphanumeric characters/symbols (e.g.!, \$, # or %)
- v. Unicode characters

Prepared By	Reviewed By	Approved By	Version 1
Susie Wall	Poppy Henderson	Mark Henderson	August 2024

vi. Cannot have the same first three characters as the username

Enforced Passwords: The Company may apply an enforced password into critical areas of the business and this password will be randomly chosen by the computer. These passwords must be memorised by the user and not amended to a personal alternative.

Password Change Intervals: The following measures are in place to enhance the Company’s password security:

- a) Users can change their passwords at any time.
- b) Employees shall change their password at least every 90 days.
- c) The Company reserves the right to enforce stipulated passwords at any time.

Virus warnings/alerts

All desk and laptop computers in use have antivirus software (including anti-spyware/malware). For the most part, the interaction between the computer and antivirus software will go unnoticed by users of the computer. On occasion, an antivirus warning message may appear on the computer screen. The message may indicate that a virus has been detected which could cause loss, theft or damage to data. The warning message may indicate that the antivirus software may not be able to rectify the problem and so must be reported to your Line Manager as soon as possible.

Media loss

Use of portable media such as CD/DVD, USB Flash sticks/HD drives for storing data requires prior permission by The Company’s Directors. The use of PCs and laptops, and many other portable devices increases the vulnerability of data. Any unauthorised user of portable or other devices may result in disciplinary action.

ID Badges

It is essential for all The Company’s customers to be able to identify our Technical Employees when they visit their premises. Therefore, the carrying and wearing ID badges is always required . Visitors to the Company’s Head Office must also be signed-in by the person managing the meeting and a visitor’s badge issued to the guest.

Data loss/disclosure

The potential for data loss applies to any data when:

- Transmitted over a network and reaching an unintended, unauthorised recipient (e.g. via email)
- Intercepted over the internet through non-secure channels
- Posted on the internet whether accidental or intentional
- Published on The Company’s website that is inaccurate or inappropriate
- Verbally disclosed
- Disclosed by employees to the press or media
- That cannot be located on the IT system or elsewhere (paper or electronic)
- On unlocked or unsecure devices
- Not collected from printers
- Left on desks or in unattended areas

All employees must act responsibly, professionally and be mindful of the importance of maintaining the security and integrity of data. Any loss of data and/or disclosure whether intentional or accidental must be reported immediately following the reporting process outlined in Section 3.3.

Personal information abuse

Any personal data such as someone’s home address, bank account, email address, phone number, etc., must not be disclosed, discussed or passed on to any individual who is not in a position of authority to view, disclose or distribute such information.

Any abuse/misuse of such person-specific data must be reported as outlined in Section 3.3 of this document.

Prepared By	Reviewed By	Approved By	Version 1
Susie Wall	Poppy Henderson	Mark Henderson	August 2024

Physical Security

Maintaining the physical security of offices and rooms where data are stored, maintained, viewed, or accessed is of paramount importance. Rooms or offices which have been designated specifically as areas where secure information is located or stored shall have a method of physically securing access to the room (swipe cards). Unsecured rooms should not be used to store sensitive and personal data.

Swipe Cards

Swipe-cards are issued to Senior Manager to restrict access to controlled rooms. Swipe-cards must not be lent to others for use. If secure room access is required by someone who does not hold a swipe-card, that person must always be accompanied by a swipe-card holder. The loss of a swipe-card must be reported immediately to HR/Office Manager.

Missing correspondence

Data which cannot be accounted for, e.g. it never arrived at its intended destination whether sent by post, electronically or for printing, must be reported (See Section 3.3).

Discovered correspondence/media

Data stored on any media or physically printed which has been found in an unsecure location or in a place where the security and integrity of the data could be compromised, shall be reported as a data security incident (see Section 3.3).

Loss or theft of IT/information

Data which can no longer be located or accounted for, e.g. it cannot be found in a location where it is expected to be or which is known or suspected to have been stolen, shall be reported as a security incident (see Section 3.3).

Company email address use

Employees must not use their company email address: -

- *To register an account on any website being used for personal reasons, or to receive communications from such websites e.g. Social networking sites such as Facebook and eBay or similar sites, message boards or any blog sites; or any non- business related site/activity.*
- *To receive communications relating to any personal businesses or income generating ventures, such as property letting.*
- *To subscribe to regular update emails for social activities such as cinema or theatre listings or other non-business purposes.*

3.2 Responsibilities

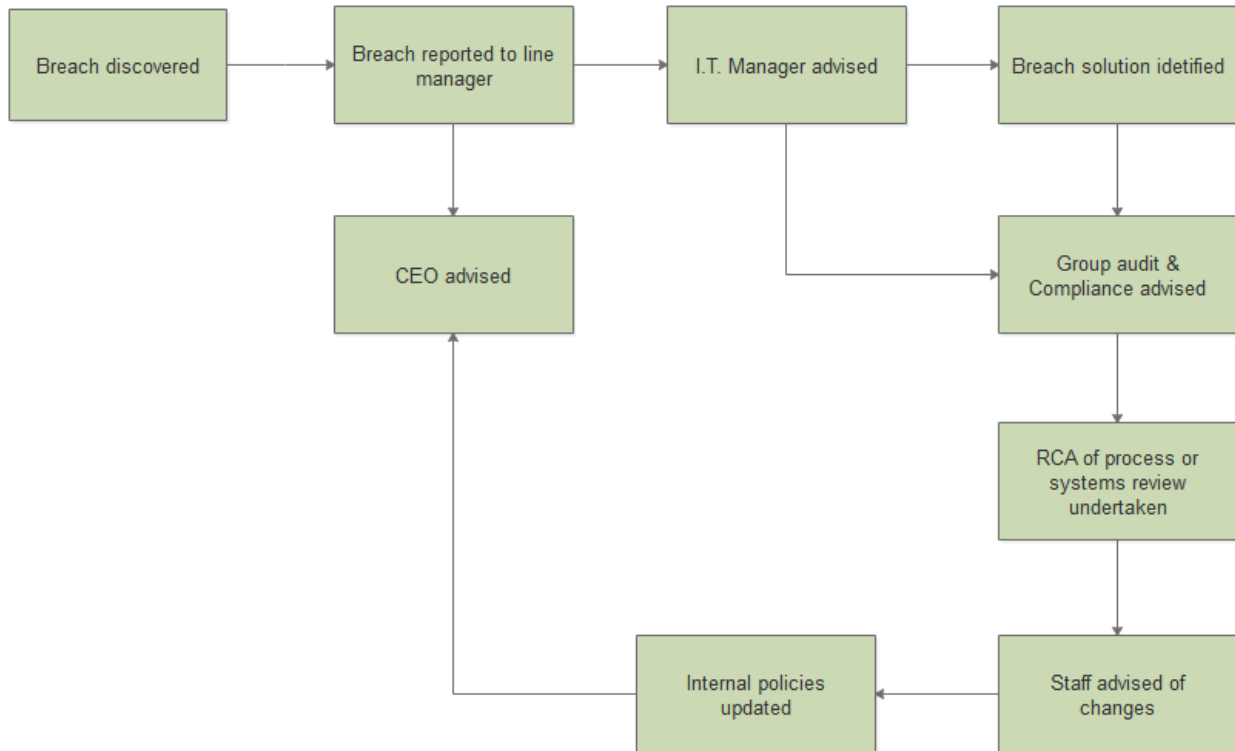
It is the responsibility of all employees and contractors who undertake work for The Company, wherever this may be, to report security incidents. The Company's Incident Reporting Process (Section 3.3 of this document) seeks to identify risks and understand and eliminate root causes that may lead to damage to the integrity and security of The Company's data and IT Systems.

It is also a responsibility of all individuals and handlers of data to ensure that all policies and procedures dealing with the security and integrity of data are followed.

Prepared By	Reviewed By	Approved By	Version 1
Susie Wall	Poppy Henderson	Mark Henderson	August 2024

1.3 Incident Reporting Process

The following diagram outlines the process to be followed for data and IT Facility incident reporting: -



Method of reporting:

Security incidents/breaches are to be reported immediately to a Line Manager, HSEQ & Compliance Manager, or a member of the Senior Management Team by telephone and/or email.

Reporting Actions and Investigations

When an incident is reported, the IT Manager will be notified. The IT Manager will log the incident and then determine if it needs to be escalated to the CEO. Investigating officers involved in reviewing IT Systems incidents and data breaches include:

- CEO
- CFO
- Head of Insurance
- HSEQ & Compliance Manager
- Contracted IT security company
- IT Manager

Investigating officers shall undertake to:

- a) Analyse and establish the immediate and root cause of the incident and take any necessary steps to prevent a recurrence.
- b) Report to all affected parties and maintain communication and confidentiality throughout the investigation.
- c) Take necessary remedial action to remedy the direct impact of the incident.
- d) Contact third parties to resolve errors/faults in software or other systems.

Prepared By	Reviewed By	Approved By	Version 1
Susie Wall	Poppy Henderson	Mark Henderson	August 2024

- e) Ensure all system logs and records are securely maintained and available to authorised personnel as and when required.
- f) Ensure only authorised personnel have access to systems and data.
- g) Ensure corrective and preventative measures are implemented and monitored for effectiveness.

Incident Log: All incidents that are logged shall record in detail the circumstances and context of the incident, including any actions arising from the investigation. Furthermore, any incident types which were initially believed to have been resolved, but have recurred, will be reopened and a new investigation initiated.

During incident investigations, hardware, logs, and records may be analysed by The Company’s IT Manager. Information and data may be gathered as evidence to support possible disciplinary or legal action. It is essential that during these investigations that confidentiality is maintained always.

On conclusion of an investigation, recommendations will be made about changes to existing policies and procedures. For those incidents arising from an employee’s behaviour or actions, disciplinary proceeding may be taken.

Data Owner/Responsibilities

Specific Responsibilities

Several employees of The Company have specific or overarching responsibilities for preserving the confidentiality, integrity and availability of data and IT Systems. These include:

The Company’s CEO/IT Manager is ultimately responsible for the review, development and enforcement of this policy and for ensuring that action is taken in the event of a security incident or incidence of non-compliance. They are also responsible for the general oversight over all IT Systems, data handling and security. Other responsibilities include:

- Ensuring that arrangements are in place internally or via third parties (e.g. IT Service Partners) for the secure storage of data.
- Ensuring audits are undertaken on GDPR compliance.
- Completing a risk assessment so that IT and data risks are fully understood.
- Determining and controlling data access rights/permissions.
- Ensuring there are appropriate backup, retention, disaster recovery and disposal mechanisms in place.
- The management of The Company’s IT Service Partners.
- Approving the revision and updating of IT Facility and data security procedures and policies.

All Employees: have responsibilities with regard the security of data. These include: -

- Securing their work area before leaving it unattended.
- Not sending/emailing confidential information to third-parties or social media via Magicman or personal email or social media accounts.
- Not sharing passwords or using passwords that are easy to guess.
- Not leaving customer data or sensitive printed material on their desks when away from their desks.
- Shredding all paperwork that is no longer required, e.g. commercially sensitive or personal customer information.
- Locking their computer before leaving it unattended (to lock: Windows logo key+L, to open: Ctrl + Alt + Del)
- Logging out of Citrix and then shutting down their computer at the end of the day.

HR Manager, Head of Finance, Operations Manager have responsibility for: -

- Ensuring that their employees follow the data handling procedures and security measures outlined in this procedure.
- Periodically reviewing and revising local data handling measures and security.
- Reporting security events to the CEO/General Manager.

IT Services Partners: have been appointed by The Company as third-party IT specialist. Their prime responsibility is to provide day-to-day technical support while also ensuring the availability and full functioning of the Company’s IT

Prepared By	Reviewed By	Approved By	Version 1
Susie Wall	Poppy Henderson	Mark Henderson	August 2024

Systems. They are also required to operate within the demands of this policy and implement best practices for IT Systems and data security.

GCI (formerly Blue Chip): is a support partner who hosts the Company’s data within a secure data centre remote from the Brighton Head Office. GCI monitor the systems 24/7 and liaise with the I.T. Manager regarding any security issues.

Big Change: hosts, supports and secures the Customer Relationship Management (CRM) platform known as ‘Job Watch’. The CRM data are held in off-site data centres. The Company’s Office Manager and the IT Manager are the principal points of contacts with Big Change.

Legal & Regulatory Obligations

The Company has a responsibility to abide by and adhere to all current UK and EU legislation as well as a variety of regulator and contractual requirements. Relevant legislation includes:

- I. The Computer Misuse Act 1990
- II. Data Protection Act 2018
- III. The Freedom of Information Act 2000
- IV. Regulation of Investigatory Powers Act 2000
- V. Copyright, Designs and Patents Act 1988
- VI. Defamation Act 1996 • Obscene Publications Act 1959
- VII. Protection of Children Act 1978 • Criminal Justice Act 1988
- VIII. Digital Economy Act 2010

Three such laws are summarised below:

The Computer Misuse Act

The **Computer Misuse Act 1990** defines offences in relation to the misuse of computers. The three principal offences of the Act are:

- a) Unauthorised access to computer material.
- b) Unauthorised access with intent to commit or facilitate commission of further offences.
- c) Unauthorised modification of computer material.

The Data Protection Act 2018 and the General Data Protection Regulation

The European Union’s (EU) General Data Protection Regulation (GDPR) became effective from the 25 May 2018. It confers greater protection and safeguards on the personal data of individuals, such as their names, email addresses, phone numbers, identification numbers. The regulation is implemented in the UK through the Data Protection Act 2018.

In addition to providing more rights and protections to individuals, it also introduces more obligations on businesses with respect to transparency, security and accountability in processing personal data. The Company is committed to ensuring that it complies with the seven key principles of Article 5 of the Regulation, which, in summary, state that personal data should be:

- i. Processed lawfully, fairly and in a transparent manner.
- ii. Collected for specified, explicit and legitimate purposes only.
- iii. Accurate and, where necessary, kept up to date.
- iv. Adequate, relevant, and limited to what is necessary.
- v. Kept in a form that permits the identification of data subject for no longer than necessary.
- vi. Processed in a manner that ensures appropriate security.

And that the controller (the Company) of such data:

- vii Shall be responsible for, and able to demonstrate, compliance.

Prepared By	Reviewed By	Approved By	Version 1
Susie Wall	Poppy Henderson	Mark Henderson	August 2024

Regulation of Investigatory Powers Act 2000

The Regulation of Investigatory Powers Act 2000 regulates the powers of public bodies to carry out surveillance and investigation. It covers the interception and use of communications data and can be invoked in the cases of national security, and for the purposes of detecting crime, preventing disorder, public safety and protecting public health.

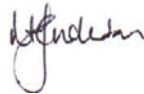
Retention of data

The below sets out the length of time different classifications of documents are kept for, after this period physical documents are shredded and disposed of using the Recycling Partnership and electronic documents will be deleted from our systems.

- HR Documents including personnel files – 6 years (plus the current year)
- Financial Documents – 6 years (plus the current year)
- Insurance Documents – 12 years (plus the current year)
- Health & Safety documents such as accidents records, RIDDOR etc – 5 years (plus the current year)
- Fleet Documents such as accident claims – 3 years (plus the current year)

Signed by: Mark Henderson CEO

Date: 01.08.2024



Prepared By	Reviewed By	Approved By	Version 1
Susie Wall	Poppy Henderson	Mark Henderson	August 2024