
CYBER SECURITY POLICY

Prepared By:

KEELAGHER OKEY ASSOCIATES LIMITED
74A London Road, Stockton Heath, Warrington, WA4 6HR

Date: 31st January 2026
Version (3.0)

Signed:



Document Control Record

Origin Date	Revision Number	Document Title	Reason for Amendment	Amendment by Amendment Date	Approved By
20/10/2023	1.0	Cyber Security Policy	Annual Review	Stuart Leak 19/10/2024	JFO
19/10/2024	2.0	Cyber Security Policy	Annual review ✓ Managing Director Derek Bradshaw added ✓ Company address changed	Stuart Leak 31/01/2026	DB
31/01/2026	3.0	Cyber Security Policy			

Table of Contents	Page
STATEMENT OF INTENT	4
PART 1 TYPES OF SECURITY BREACHES & CAUSES	4
PART 2 ROLES & RESPONSIBILITIES	5
PART 3 SECURE CONFIGURATION	7
PART 4 NETWORK SECURITY	8
PART 5 MALWARE PREVENTION	9
PART 6 USER PRIVILEGES & PASSWORDS	10
PART 7 REMOVEABLE MEDIA CONTROLS	11
PART 8 HOME WORKING	12
PART 9 BACKING UP DATA	13
PART 10 AVOIDING PHISING ATTACKS	14
PART 11 USER TRAINING & AWARENESS	15
PART 12 CYBER-SECURITY INCIDENTS	16
PART 13 ASSESSMENTS OF RISKS	18
PART 14 CONSIDERATION OF FURTHERE NOTIFICATION	18
PART 15 EVALUATION	19
PART 16 MONITORING & REVIEW	19

STATEMENT OF INTENT

KEELAGHER OKEY ASSOCIATES LTD is committed to maintaining the confidentiality, integrity and availability of its information and ensuring that the details of the finances, operations and individuals within the organisation are only accessible to the appropriate individuals. It is, therefore, important to implement appropriate levels of access, uphold high standards of security, take suitable precautions, and have systems and procedures in place that support this.

We recognise, however, that breaches in security can occur. In industry, most breaches are caused by human error, so the practice will ensure all staff are aware of how to minimise this risk. In addition, because most information is stored online or on electronic devices that can be vulnerable to cyberattacks, we will ensure there are procedures in place to prevent attacks occurring. To minimise both risks, it is necessary to have a contingency plan containing a procedure to minimise the potential negative impacts of any security breach and to take steps to help prevent a repeat occurrence.

PART 1 | TYPES OF SECURITY BREACH AND CAUSES

Unauthorised use without damage to data – involves unauthorised persons accessing data on the KEELAGHER OKEY ASSOCIATES LTD system, e.g. ‘hackers’, who may read the data or copy it, but who do not actually damage the data in terms of altering or deleting it. This includes unauthorised people within KEELAGHER OKEY ASSOCIATES LTD, e.g. where workers or visitors access systems that staff have left open and/or logged in, or where staff access data beyond their authorisation.

Unauthorised removal of data: involves an authorised person accessing data, who removes the data to pass it on to another person who is not authorised to view it, e.g. a staff member with authorised access who passes the data on to a friend without authorised access. This is also known as data theft. The data may be forwarded or deleted altogether.

Damage to physical systems: involves damage to the hardware in KEELAGHER OKEY ASSOCIATES LTD’s ICT system, which may result in data being inaccessible to the practice and/or becoming accessible to unauthorised persons.

Unauthorised damage to data: involves an unauthorised person causing damage to data, either by altering or deleting it. Data may also be damaged by a virus attack, rather than a specific individual.

Breaches in security may be caused by the actions of individuals, and may be accidental, malicious or the result of negligence:

- Accidental breaches can occur as a result of human error or insufficient training for staff, so they are unaware of the procedures to follow.

- Malicious breaches can occur as a result of a hacker wishing to cause damage to the practice through accessing and altering, sharing or removing data.
- Negligence can occur as a result of a staff member knowingly disregarding KEELAGHER OKEY ASSOCIATES LTD policies and procedures or allowing persons to access data without authorisation and/or supervision.

Breaches in security may also be caused by system issues, which could involve incorrect installation, configuration problems or operational errors:

- The incorrect installation of antivirus software and/or use of outdated software can make the practice software more vulnerable to a virus.
- Incorrect firewall settings being applied, e.g. unrestricted access to the practice network, can allow unauthorised individuals to access the KEELAGHER OKEY ASSOCIATES LTD system.
- Operational errors, such as confusion between back-up copies of data, can cause the most recent data to be overwritten.

PART 2 | ROLES AND RESPONSIBILITIES

The Director will be responsible for:

- Ensuring the practice has appropriate cyber-security measures in place.
- Ensuring the practice has an appropriate approach to managing data breaches in place.
- Supporting the Head of Professional Services and other relevant staff in the delivery of this policy.

The Head of Operations (HoPS) will be responsible for:

- Ensuring all staff members and contractors are aware of their responsibilities in relation to this policy.
- Ensuring appropriate user access procedures are in place.
- Responding to alerts for access to inappropriate content in line with the Online Safety Policy.
- Organising training for staff members in conjunction with the Head of Operations.
- Ensuring a log of cyber-security incidents is maintained.

The Head of Operations (HoOp) will be responsible for:

- The overall monitoring and management of data security.
- Deciding which strategies are required for managing the risks posed by internet use.
- Leading on the practice's response to incidents of data security breaches.
- Assessing the risks to the practice in the event of a cyber-security breach.
- Producing a comprehensive report following a full investigation of a data security breach.
- Determining which organisations and individuals need to be notified following a data security breach, and ensuring they are notified.

- Working with the IT Support Manager (ITSM) and HoPS after a data security breach to determine where weaknesses lie and improve security measures.
- Organising training for staff members on data security, network security and preventing breaches.
- Monitoring and reviewing the effectiveness of this policy, alongside the HoPS, and communicating any changes to staff members.

The IT Support Manager will be responsible for:

- Maintaining an inventory of all ICT hardware and software currently in use at the practice.
- Ensuring any out-of-date software is removed from the KEELAGHER OKEY ASSOCIATES LTD systems.
- Setting up user privileges in line with recommendations from the HoPS.
- Removing any inactive users from the practice system and ensuring that this is always up-to-date.
- Installing appropriate security software on staff members' personal devices where the HoPS has permitted for them to be used for work purposes.
- Ensuring all KEELAGHER OKEY ASSOCIATES LTD-owned devices have secure malware protection and are regularly updated.
- Recording any alerts for access to inappropriate content and notifying the HoPS.
- Leading the cyber security recovery team in response to any incidents

Optimised IT will be responsible for:

- Implementing effective firewalls to enhance network security and ensuring that these are monitored regularly.
- Installing, monitoring and reviewing filtering systems for the KEELAGHER OKEY ASSOCIATES LTD network.
- Performing a back-up of all electronic data held by the practice, ensuring detailed records of findings are kept.

All staff members will be responsible for:

- Understanding their responsibilities in regard to this policy.
- Undertaking the appropriate training.
- Ensuring they are aware of when new updates become available and how to safely install them.

PART 3 | SECURE CONFIGURATION

An inventory will be kept of all ICT hardware and software currently in use at the practice, including mobile phones and other personal devices provided by KEELAGHER OKEY ASSOCIATES LTD. The inventory will be stored in the asset database and will be audited on an annual basis to ensure it is up-to-date. Any changes to the ICT hardware or software will be documented using the asset database and will be authorised by the HoPS before use.

All systems will be audited regularly to ensure the software is up-to-date. Any new versions of software or new security patches will be added to systems, ensuring that they do not affect network security, and will be recorded in the inventory. Any software that is out-of-date or reaches its 'end of life' will be removed from systems, e.g. when suppliers end their support for outdated products, meaning that the product is not able to fulfil its purpose anymore.

All hardware, software and operating systems will require passwords for individual users before use. The practice believes that locking down hardware, such as through the use of strong passwords, is an effective way to prevent access by unauthorised users.

The practice will consider referring to the five security controls outlined in the National Cyber Security Centre's (NCSC's) 'Cyber Essentials'. These are:

- **Firewalls:** Firewalls function as a barrier between internal networks and the internet. They will be installed on any device that can access the internet, particularly where staff are using public or otherwise insecure Wi-Fi.
- **Secure configuration:** The default configurations on devices and software are often as open as possible to ensure ease of use, but they also provide more access points for unauthorised users. The practice will disable or remove any unnecessary functions and change default passwords to reduce the risk of a security breach.
- **Access control:** The more people have access to data, the larger the chance of a security breach. The practice will ensure that access is given on a 'need-to-know' basis to help protect data. All accounts will be protected with strong passwords, and where necessary, two-factor authorisation.
- **Malware protection:** The practice will protect itself from malware by installing antivirus and anti-malware software.
- **Patch management:** The practice will install software updates as soon as they are available to minimise the time frame in which vulnerabilities can be exploited. If the manufacturer stops offering support for the software, the practice will replace it with a more up-to-date alternative.

PART 4 | NETWORK SECURITY

In line with the UK GDPR, the practice will appropriately test, assess, and evaluate any security measures put in place regularly to ensure these measures remain effective.

The practice will employ firewalls in order to prevent unauthorised access to the systems.

Localised firewall deployment

The practice's firewall will be deployed as a localised deployment, which means the broadband service connects to a firewall that is located on an appliance or system on the practice premises, as either discrete technology or a component of another system.

It is the responsibility of the Optimised IT to effectively manage the firewall. Optimised IT will ensure that:

The firewall is checked regularly for any changes and/or updates, and that these are recorded using the inventory.

- Any changes and/or updates that are added to servers, including access to new services and applications, are checked to ensure that they do not compromise the overall network security.
- The firewall is also checked regularly to ensure that a high level of security is maintained, and there is effective protection from external threats.
- Any compromise of security through the firewall is reported to the HoPS and HoOP, who will ensure that it is recorded. The IT Manager will react appropriately to security threats to find new ways of managing the firewall.

PART 5 | MALWARE PREVENTION

The practice understands that malware can be damaging for network security and may enter the network through a variety of means, such as email attachments, social media, malicious websites or removable media controls.

The IT Manager will ensure that all practice devices have secure malware protection and undergo regular malware scans in line with specific requirements. The IT Manager will update malware protection on a regular basis to ensure it is up-to-date and can react to changing threats. Malware protection will also be updated in the event of any attacks to the practice's hardware and software.

The practice will use mail security technology, which will detect and block any malware that is transmitted by email. This will also detect any spam or other messages which are designed to exploit users. The IT Manager will review the mail security technology on a regular basis to ensure it is kept up-to-date and effective.

Staff members are only permitted to download apps on any KEELAGHER OKEY ASSOCIATES LTD-owned device from manufacturer-approved stores and with prior approval from the HoPS. Where apps are installed, the IT Manager will keep up-to-date with any updates, ensuring staff are informed of when updates are ready and how to install them.

PART 6 | USER PRIVILEGES AND PASSWORDS

The practice understands that controlling what users have access to is important for promoting network security and data protection. User privileges will be differentiated, e.g. managers will have different access to data and the network than other members of staff, whose access will also be role-based.

The HoPS will decide what users have access to and will communicate this to the IT Manager. The IT Manager will ensure that user accounts are set up to allow users access to the information required, in line with the HoPS's instructions, whilst minimising the potential for deliberate or accidental attacks on the network.

All users will be required to change their passwords if they become known to other individuals, in line with the 'Secure configuration' section of this policy. Staff members are responsible for remembering their passwords. Multi-factor authentication (multiple different methods of verifying the user's identity) should be used wherever possible.

A multi-user account will be created for visitors to the practice, such as volunteers, and access will be filtered as per the HoPS instructions. Usernames and passwords for this account will be changed on a termly basis and will be provided as required.

KEELAGHER OKEY ASSOCIATES LTD will manually delete inactive users or users who have left the practice. The IT Manager will manage this provision to ensure that all users that should be deleted are, and that they do not have access to the system.

The IT Manager will review the password system on a regular basis to ensure it is working at the required level.

PART 7 | REMOVABLE MEDIA CONTROLS

The practice understands that contractors and staff may need to access the KEELAGHER OKEY ASSOCIATES LTD network from outside the practice premises. Effective security management will be established to prevent access to, or leakage of, data, as well as any possible risk of malware.

The IT Manager will encrypt all KEELAGHER OKEY ASSOCIATES LTD-owned devices for personal use, such as laptops, USB sticks, and tablets, to ensure that they are password protected. If any portable devices are lost, this will prevent unauthorised access to personal data.

Before distributing any KEELAGHER OKEY ASSOCIATES LTD-owned devices, the IT Manager will ensure that manufacturers' default passwords have been changed. A set password will be chosen, and the staff member will be prompted to change the password once using the device. The IT Manager will check KEELAGHER OKEY ASSOCIATES LTD-owned devices on a regular basis to detect any unchanged default passwords.

If contractors and staff are instructed that they are able to use their personal devices, they will ensure that they have an appropriate level of security and firewall to prevent any compromise of the practice's network security. Any device which is configured for use with a KEELAGHER OKEY ASSOCIATES LTD email will be password or passcode protected.

When using laptops, tablets and other portable devices, the HoPS will determine the limitations for access to the network, as described in the 'Network security' section of this policy.

Staff will avoid connecting to unknown Wi-Fi hotspots, such as in coffee shops, when using any KEELAGHER OKEY ASSOCIATES LTD-owned laptops, tablets or other devices, or when accessing KEELAGHER OKEY ASSOCIATES LTD networks.

The Wi-Fi network at the practice will be password protected and will only be given out as required.

PART 8 | HOME WORKING

Staff and contractors will adhere to data protection legislation and the practice's related policies when working remotely.

Staff will receive annual briefing regarding what to do if a data protection issue arises from any home working.

Wherever possible, personal data will not be taken home by staff members for the purposes of home working, due to the risk of data being lost or the occurrence of a data breach.

Staff and contractors may be required to use their own devices for the duration of remote working. Using a shared personal or household device for practice purposes should be avoided where possible.

Staff and contractors are not permitted to let their family members or friends use any KEELAGHER OKEY ASSOCIATES LTD equipment, in order to protect the confidentiality of any personal data held on the device. Any staff member found to have shared personal data without authorisation will be disciplined in line with the Disciplinary Policy and Procedure.

Staff who require access to personal data to enable them to work from home will first seek approval from the HoPS, and it will be ensured that the appropriate security measures are in place by the IT Manager and the HoOP, e.g. secure passwords and anti-virus software.

Staff will be informed that caution should be exercised while accessing personal data if an unauthorised person is in the same room. If a member of staff needs to leave their device unattended, the device should be locked.

Personal data should only be transferred to a home device if this is necessary for the member of staff to carry out their role. When sending confidential information, staff must never save confidential information to a personal or household device. Data that is transferred from a work to a home device will be encrypted so that if any data is lost, stolen or subject to unauthorised access, it will remain safe until it can be recovered.

To ensure reasonable precautions are taken when managing data, staff will avoid:

- Keeping personal data on unencrypted hard drives.
- Sending work emails to and from personal email addresses.
- Leaving logged-in devices and files unattended.
- Using shared home devices where other household members can access personal data.
- Using an unsecured Wi-Fi network.

Staff working from home will be encouraged and enabled to go paperless, where possible, as paper files cannot be protected digitally and may be misplaced. If sensitive data is taken off the practice premises to allow staff to work from home, it will be transported in a lockable bag or container. The practice's procedures for taking data off the premises will apply to both paper-based and electronic data.

When taking physical copies of data, e.g. paper documents and non-assigned KEELAGHER OKEY ASSOCIATES LTD-owned devices, off the practice premises, staff will sign out the documents from the Office Manager. The physical data will be signed back in when staff return it.

Any devices that are used by staff and contractors for remote working and will be assessed by the IT Manager prior to being taken to the home setting, using the following checks:

- System security check – the security of the network and information systems
- Data security check – the security of the data held within the systems
- Online security check – the security of any online service or system, e.g. the KEELAGHER OKEY ASSOCIATES LTD website
- Device security check – the security of the personal device, including any ‘bring your own device’ systems

The IT Manager will provide staff and contractors with details and instructions for accessing the KEELAGHER OKEY ASSOCIATES LTD network that they will be using throughout the duration of their remote working.

In the event that a staff member or contractor decides to leave the practice permanently, all data in any form will be returned on or before their last day.

PART 9 | BACKING UP DATA

Optimised IT performs a back-up of all electronic data held by the practice monthly, and the date of the back-up is recorded using a log.

Where possible, back-ups are run overnight and are completed before the beginning of the next working day. Upon completion of back-ups, data is stored on KEELAGHER OKEY ASSOCIATES LTD’s hardware, which is password protected. Only authorised personnel will be able to access back-ups of the practice’s data.

The practice’s back-up strategy will be tested on a regular basis.

PART 10 | AVOIDING PHISING ATTACKS

The IT Manager will configure all staff accounts using the principle of 'least privilege' – staff members are only provided with as much rights as are required to perform their jobs.

Designated individuals who have access to the master user account will avoid browsing the web or checking emails whilst using this account. Two-factor authentication is used on any important accounts, such as the master user account, or any key accounts, such as the HoPS and HoOP.

Staff will use the following warning signs when considering whether a communication may be unusual:

- Is it from overseas?
- Is the spelling, grammar and punctuation poor?
- Is the design and quality what you would expect from a large organisation?
- Is it addressed to a 'valued customer', 'friend' or 'colleague'?
- Does it contain a veiled threat that asks the staff member to act urgently?
- Is it from a senior member of the practice asking for a payment?
- Is it from a supplier advising of a change in bank account details for payment?
- Does it sound too good to be true? It is unlikely someone will want to give another individual money or access to another service for free.
- Is it from a generic email address, such as Gmail or Hotmail?

The IT Manager will ensure that an appropriate email filtering system is used to identify which emails would be classed as junk or spam, applied in accordance with the 'Malware prevention' section of this policy. The IT Manager will ensure that the filtering system is neither too strict nor too lenient, to allow the correct emails to be sent to the relevant folders.

To prevent anyone having access to unnecessary personal information, the HoOP and HoPS will ensure the practice's social media accounts and websites are reviewed on a regular basis, making sure that only necessary information is shared.

The HoPS will ensure contractors and staff are aware of acceptable use of social media and the information they share about the practice and themselves.

PART 11 | USER TRAINING AND AWARENESS

The IT Manager and HoPS will arrange training for contractors and staff on a regular basis to ensure they are aware of how to use the network appropriately. This will cover identifying irregular methods of communication in order to help staff members spot requests that are out of the ordinary, such as receiving an invoice for a service not used, and who to contact if they notice anything unusual. Unusual communications could come in a variety of forms, e.g. emails, phone calls, text messages or social media messages.

The HoPS will arrange for staff and contractors to undertake the appropriate training relating to online safety issues.

The HoPS will also arrange training for pupils and staff on a regular basis on maintaining data security, preventing data breaches, and how to respond in the event of a data breach. Training for all staff members will be arranged by the It Manager and HoOP within two weeks following an attack, breach or significant update.

Through training, all contractors and staff will be aware of who they should inform first in the event that they suspect a security breach, and who they should inform if they suspect someone else is using their passwords. All staff will receive training as part of their induction programme. All contractors will receive training upon joining the practice.

All users will be made aware of the disciplinary procedures for the misuse of the network leading to malicious attacks, in accordance with the process detailed in the Behavioural Policy and the Disciplinary Policy and Procedure.

PART 12 | CYBER-SECURITY INCIDENTS

All cyber-security incidents will be managed in line with the practice's Cyber Response and Recovery Plan.

Any individual that discovers a cyber-security incident will report this immediately to the HoPS and the HoOP. Either the HoPS or HoOP will inform the IT Manager.

When an incident is raised, the HoOP will record the following information:

- Name of the individual who has raised the incident
- Description and date of the incident
- Description of any perceived impact
- Description and identification codes of any devices involved, e.g. KEELAGHER OKEY ASSOCIATES LTD-owned laptop
- Location of the equipment involved
- Contact details for the individual who discovered the incident
- Whether the incident needs to be reported to the relevant authorities, e.g. the ICO or police

The practice's HoOP will take the lead in investigating the incident, with assistance from the IT Manager, and will be allocated the appropriate time and resources to conduct this. The HoOP, as quickly as reasonably possible, will ascertain the severity of the incident and determine if any personal data is involved or has been compromised. The HoOP will oversee a full investigation and produce a comprehensive report. The cause of the incident, and whether it has been contained, will be identified – ensuring that the possibility of further loss or jeopardising of data is eliminated or restricted as much as possible.

If the HoOP determines that the severity of the security breach is low, the incident will be managed in accordance with the following procedures:

- In the event of an internal breach, the incident is recorded using an incident log, and by identifying the user and the website or service they were trying to access
- The HoPS will issue disciplinary sanctions to the contractor or member of staff who caused the breach, in accordance with the Disciplinary Policy and Procedures
- In the event of any external or internal breach, the IT Manager will record this using an incident log and respond appropriately, e.g. by updating the firewall, changing usernames and passwords, updating filtered websites or creating further back-ups of information
- The practice will organise updated staff training following a breach
- Any further action which could be taken to recover lost or damaged data will be identified – this includes the physical recovery of data, as well as the use of back-ups

Where the security risk is high, the HoOP will establish what steps need to be taken to prevent further data loss, which may require support from various staff. This action will include:

- Informing relevant staff of their roles and responsibilities in areas of the containment process.
- Taking systems offline.
- Retrieving any lost, stolen or otherwise unaccounted for data.
- Restricting access to systems entirely or to a small group.
- Backing up all existing data and storing it in a safe location.
- Reviewing basic security, including:
 - Changing passwords and login details on electronic equipment.
 - Ensuring access to places where electronic or hard data is kept is monitored and requires authorisation.

Where appropriate, e.g. if offences have been committed under the Computer Misuse Act 1990, the HoOP will inform the police of the security breach.

Where the practice has been subject to online fraud, scams or extortion, the HoOP will also report this using the Action Fraud website.

The IT Manager will test all systems to ensure they are functioning normally, and the incident will only be deemed 'resolved' when it has been assured that the practice's systems are safe to use.

13 | ASSESSMENT OF RISKS

The following questions will be considered by the HoOP to fully and effectively assess the risks that the cyber-security breach has brought, and to help take the next appropriate steps. All relevant questions will be clearly and fully answered in the HoOP's report, which should record:

- What type of, and how much, data is involved?
- How sensitive is the data? Sensitive data is defined in the UK GDPR; some data is sensitive because of its very personal nature (e.g. health records) while other data types are sensitive because of what might happen if it is misused (e.g. bank account details).
- Is it possible to identify what has happened to the data – has it been lost, stolen, deleted or tampered with?
- If the data has been lost or stolen, were there any protective measures in place to prevent this, such as data and device encryption?
- If the data has been compromised, have there been effective measures in place that have mitigated the impact of this, such as the creation of back-ups and spare copies?
- Has individuals' personal data been compromised – how many individuals are affected?
- Who are these individuals – are they contractors, staff, volunteers, suppliers?
- Could their information be misused or manipulated in any way?
- Could harm come to individuals? This could include risks to the following: - Physical safety - Emotional wellbeing - Reputation - Finances - Identity - Private affairs becoming public
- Are there further implications beyond the risks to individuals? Is there a risk of loss of confidence and/or damage to the practice's reputation, or risk to the practice's operations?
- Who could help or advise the practice on the breach?

PART 14 | CONSIDERATION OF FURTHER NOTIFICATION

The HoOP will consider whether there are any legal, contractual or regulatory requirements to notify individuals or organisations that may be affected or who will have an interest in data security.

The HoOP will assess whether notification could help the individual(s) affected, and whether the individual(s) could act on the information provided to mitigate risks, e.g. by cancelling a credit card or changing a password.

The HoOP will consider who to notify, what to tell them and how they will communicate the message, which may include:

- A description of how and when the breach occurred and what data was involved.
- Details of what has already been done to respond to the risks posed by the breach.

- Specific and clear advice on the steps they can take to protect themselves, and what the practice is willing to do to help them.
- A way in which they can contact the practice for further information or to ask questions about what has occurred.

The HoOP will consider, as necessary, the need to notify any third parties, such as the police, insurers, professional bodies, website and/or system owners, banks and/or credit card companies, who can assist in helping or mitigating the impact on individuals.

PART 15 | EVALUATION

The HoOP will document all the facts regarding the breach, its effects and the remedial action taken. This should be an evaluation of the breach, and what actions need to be taken forward.

The HoOP will consider the data and contexts involved, establish the root of the breach, and where any present or future risks lie, taking into consideration whether the breach is a result of human or systematic error and see how a recurrence can be prevented.

The HoOP and HoPS will identify any weak points in existing security measures and procedures. The HoOP will work with the IT Manager to improve security procedures wherever required. The HoOP and HoPS will identify any weak points in levels of security awareness and training.

The HoOP will report on findings and, with the approval of the Senior Management Team, implement the recommendations of the report after analysis and discussion.

PART 16 | MONITORING AND REVIEW

This plan will be reviewed by the Senior Management Team on an annual basis.



Name: Derek Bradshaw
Position: Managing Director
Date: 31st January 2026