Crystal Health Group Policy

Information Security Policy

1. Purpose

Crystal Health Group Limited is committed to protecting the confidentiality, integrity and availability of the information it processes.

This policy establishes the principles and responsibilities used to protect personal, commercial and operational information from accidental or unlawful loss, alteration, destruction, disclosure, misuse or unauthorised access.

It supports the secure provision of Crystal Health Group's DNA testing, drug and alcohol testing, occupational health and associated business services. It also supports the prevention, detection, management and reduction of information security incidents and provides assurance to clients, staff, suppliers and other stakeholders.

2. Scope

This policy applies to:

- All Crystal Health Group directors, employees, temporary workers and contractors.
- All information created, received, processed, stored or transmitted by Crystal Health Group.
- All systems, devices, networks, applications, records and physical locations used for Crystal Health Group business.
- External service providers where they process Crystal Health Group information or have access to its systems.

Directors, employees and contractors working under Crystal Health Group's control must comply with this policy and the supporting Information Security Management System procedures.

External service providers must comply with applicable legal and regulatory requirements and any information security requirements agreed in their contract or other written agreement with Crystal Health Group. They are not required to operate under Crystal Health Group's internal policies unless this has been expressly agreed and is appropriate to the services provided.

2.1 ISO/IEC 27001:2022

ISO/IEC 27001:2022, including its Annex A organisational, people, physical and technological controls, provides the principal framework for Crystal Health Group's Information Security Management System.

The framework enables Crystal Health Group to:

- Apply information security controls consistently across the business.
- Identify and manage information security risks.
- Define proportionate security requirements for contracts and supplier relationships.
- Monitor and assess the effectiveness of its controls.
- Demonstrate that appropriate measures are in place to protect the confidentiality, integrity and availability of information and supporting systems.

The detailed controls adopted by Crystal Health Group are recorded in its Information Security Risk Assessment, Statement of Applicability and supporting ISMS procedures and records.

3. Responsibilities

Company Directors are responsible for:

- Approving this policy and providing overall accountability for information security.
- Ensuring that appropriate resources and organisational arrangements are available.
- Reviewing significant information security risks and incidents.

The ISMS Manager is responsible for:

- The implementation and ongoing management of the Information Security Management System.
- Maintaining the Information Security Risk Assessment and Statement of Applicability.
- Coordinating policy review, monitoring and continual improvement.

The Director of Quality and Compliance is responsible for:

- Managing information security incidents through the Quality Incident Reporting process.
- Supporting investigations, corrective actions and regulatory reporting.
- Monitoring compliance and raising policy change requests where required.

Function Head Directors are responsible for:

- Implementing applicable controls within their areas.
- Managing staff access, equipment and information appropriately.
- Ensuring staff complete required training and report incidents promptly.

All staff and contractors working under Crystal Health Group's control are responsible for:

- Complying with this policy and relevant supporting procedures.
- Protecting information and equipment provided to them.
- Reporting suspected incidents, weaknesses, loss or unauthorised disclosure immediately.

3.1 Information Security Roles

Crystal Health Group assigns clear responsibility for the implementation, management and oversight of its Information Security Management System. The principal responsibilities are set out below.

Responsibility	Responsible person(s)
Overall ISMS accountability	Company Directors
ISMS management and coordination	Company Director acting as ISMS Manager
Access provisioning and termination	Company Director / Director of Operations
Device assignment and recovery	Director of Operations
Incident reporting	All staff and contractors
Incident investigation and escalation	Director of Quality and Compliance / Company Director
Policy review and approval	Company Directors
Supplier due diligence and assurance	Director of Quality and Compliance

Responsibilities are communicated during induction, relevant role training and annual refresher training.

External service providers receive the security requirements relevant to the services they provide through contracts, specifications or other written communications. They are not routinely issued with Crystal Health Group's internal operational policies.

4. Policy

This section sets out the operational, technical and organisational controls used by Crystal Health Group to protect its information, systems, equipment and premises. These controls are supported by the Information Security Risk Assessment, Statement of Applicability and relevant procedures and records.

4.1 Data Protection

Crystal Health Group processes personal data in accordance with the UK GDPR, Data Protection Act 2018, Data (Use and Access) Act 2025 and other applicable data protection legislation.

Crystal Health Group is registered with the Information Commissioner's Office under registration number **ZA260675**.

Depending on the activity involved, Crystal Health Group may act as either:

- **A Data Controller**, where it determines why and how personal data is processed; or
- **A Data Processor**, where it processes personal data on the documented instructions of another Data Controller.

Certain laboratories, occupational health providers and other professional service providers may act as independent Data Controllers. In those circumstances, they are responsible for complying with their own legal, regulatory and professional obligations.

Crystal Health Group's Privacy Policy explains how personal data is collected, used, shared, protected and retained, together with the rights available to individuals. The current policy is available at:

https://www.crystal-health.co.uk/privacy-policy/

Crystal Health Group uses approved third-party systems and service providers for activities including appointment coordination, order processing, case management, results reporting, communications and financial control.

Third-party systems and providers are subject to proportionate due diligence, contractual requirements and ongoing supplier assurance. Where a provider processes personal data on behalf of Crystal Health Group, appropriate data-processing terms are established. Where a provider acts as an independent Data Controller, its respective responsibilities are recorded or otherwise made clear.

The information security controls applying to systems, suppliers and processing activities are documented within the Information Security Risk Assessment, Statement of Applicability and supporting ISMS records.

4.2 Personal Data Breach Management

Due to the nature and sensitivity of the information processed by Crystal Health Group, all actual or suspected personal data breaches must be identified, reported, assessed and managed promptly.

All personal data breaches and suspected breaches are managed through the Quality Incident Reporting process. This provides a documented record of the incident, investigation, risk assessment, decisions, notifications, corrective actions and final outcome.

What is a Personal Data Breach?
A personal data breach is a security breach resulting in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

A breach may affect the confidentiality, integrity or availability of personal data. It may result from an accidental or deliberate act and does not need to involve the permanent loss of information.

Examples include:

- Personal data being sent to an incorrect recipient.
- Unauthorised access to a system, account, case file or physical record.
- The loss or theft of a device or document containing personal data.
- Personal data being altered, corrupted or deleted without authority.
- Information being made unavailable through system failure, ransomware or accidental deletion.
- The inappropriate disclosure of information verbally, electronically or in writing.
- A service provider experiencing an incident affecting personal data processed for Crystal Health Group.

Immediate Reporting
All staff and contractors working under Crystal Health Group's control must report an actual or suspected personal data breach to the Director of Quality and Compliance or a Company Director immediately.

The person identifying the incident should, where it is safe and appropriate to do so:

- Take reasonable steps to prevent further disclosure or loss.
- Preserve relevant evidence.
- Record when and how the incident was identified.
- Avoid deleting, altering or concealing relevant information.
- Avoid contacting affected individuals or external organisations unless authorised to do so.

Incidents must not be investigated or concluded by unauthorised personnel.

Response Plan
The following process applies to all actual or suspected personal data breaches:

1. The incident must be reported immediately to the Director of Quality and Compliance or a Company Director.

2. Immediate containment measures must be considered and implemented where appropriate.
3. A Quality Incident Report must be created to record and track the incident.
4. The facts of the incident must be established, including:
    a. What happened and when.
    b. The systems, records and people involved.
    c. The categories and approximate volume of personal data affected.
    d. The approximate number of individuals affected.
    e. Whether the information has been recovered, accessed, copied or disclosed.
    f. Any immediate action already taken.
5. Crystal Health Group's role in the affected processing must be established, including whether it is acting as a Data Controller or Data Processor.
6. A documented risk assessment must be completed to determine:
    a. The likelihood and severity of harm to individuals.
    b. Whether the relevant Data Controller must be notified.
    c. Whether the Information Commissioner's Office must be notified.
    d. Whether affected individuals must be informed.
    e. Whether any other regulator, client, insurer, professional body or law-enforcement agency should be notified.
7. Appropriate corrective and preventative actions must be identified, assigned and monitored.
8. All decisions, notifications, actions and supporting evidence must be recorded within the Quality Incident Report.
9. The Director of Quality and Compliance or a Company Director must formally review and close the incident once the investigation and required actions have been completed.

Responsibility and Escalation

The Director of Quality and Compliance is responsible for coordinating the investigation, maintaining the Quality Incident Report and ensuring that required actions are completed.

A Company Director must be informed promptly where:

- Special-category or criminal-offence data is involved.
- A large number of individuals or records may be affected.
- There is a potential risk of significant harm.
- The incident involves a cyberattack, deliberate wrongdoing or criminal activity.
- Regulatory notification may be required.

- The incident could materially affect Crystal Health Group's operations, reputation or contractual obligations.

Technical, legal, professional or regulatory advice must be obtained where appropriate.

Risk Assessment
The risk assessment must consider the potential physical, financial, material and non-material consequences for the affected individuals.

Relevant factors include:

- The nature, sensitivity and volume of the data.
- Whether special-category or criminal-offence data is involved.
- The ease with which individuals can be identified.
- The number and characteristics of the individuals affected.
- Who has obtained or may obtain access to the information.
- Whether the information was encrypted or otherwise protected.
- The likelihood that the information has been or will be misused.
- The possible consequences for the affected individuals.
- The effectiveness of containment and recovery measures.

The risk-assessment factors set out above must be considered in every case, with the outcome and supporting rationale recorded in the Quality Incident Report.

Notification to the Information Commissioner's Office
Where a personal data breach is likely to result in a risk to the rights and freedoms of individuals, Crystal Health Group must notify the Information Commissioner's Office without undue delay and, where feasible, within 72 hours of becoming aware of the breach.

Where notification is made after 72 hours, the reasons for the delay must be documented and provided to the Information Commissioner's Office.

An initial notification must not be delayed solely because all details are not yet available. Further information may be provided in phases without undue further delay.

The current ICO breach-reporting service and guidance are available at:

https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/

Informing Affected Individuals
Where a personal data breach is likely to result in a high risk to the rights and freedoms of individuals, those individuals must be informed directly and without undue delay.

The communication must use clear and plain language and include:

- A description of the nature of the breach.
- The name and contact details of the Data Protection Officer or other contact point.
- The likely consequences of the breach.
- The measures taken or proposed to address it.
- Appropriate advice about steps the individual can take to protect themselves.

Communications must be approved by the Director of Quality and Compliance or a Company Director and sent using an appropriate and secure method.

Data Controllers, Data Processors and Service Providers
Where Crystal Health Group acts as a Data Processor, it must inform the relevant Data Controller of a personal data breach without undue delay and provide reasonable assistance to enable the controller to meet its obligations.

Where a processor acting on behalf of Crystal Health Group experiences a breach, it must notify Crystal Health Group without undue delay in accordance with the applicable data-processing agreement.

Where a laboratory, occupational health provider or other professional provider acts as an independent Data Controller, it is responsible for assessing and reporting the breach under its own legal, regulatory and professional obligations. It must also notify Crystal Health Group where required by contract or where the incident materially affects shared services or individuals.

Recording and Review
All personal data breaches must be documented, including those that do not require notification to the ICO or affected individuals.

- The record must include:
- The facts and circumstances of the breach.
- Its effects and potential consequences.
- The risk assessment undertaken.
- The decision on whether notification was required.
- Containment, corrective and preventative actions.
- Communications with affected parties, clients, providers or regulators.
- The final outcome and closure approval.

Lessons learned must be considered as part of the incident review and used to improve training, systems, procedures and controls where appropriate.

4.3 Passwords, Authentication and Case Security

Crystal Health Group uses passwords, authentication controls and identity verification to prevent unauthorised access to systems, documents and client information. Controls must be proportionate to the sensitivity of the information and the risk associated with unauthorised access or disclosure.

Password Creation
Passwords used for company systems and applications must:

- Be unique to the relevant account.
- Contain at least 12 characters where the system permits.
- Use three or more random, unrelated words or be generated using an approved password manager.
- Not contain easily guessed personal information, common phrases, sequences or predictable substitutions.
- Not be reused across different systems or accounts.
- Meet any stronger requirements imposed by the relevant system or service provider.

Multi-factor authentication must be enabled wherever it is available and appropriate.

Passwords do not need to be changed routinely unless required by the relevant system, there is reason to believe the password has been compromised, or a security review identifies that a change is necessary.

Password Handling

Personnel must not:

- Disclose their password to another person.
- Store passwords in unsecured documents, emails, notebooks or other accessible locations.
- Send a password in the same communication as the document or information it protects.
- Use another person's account or allow another person to use their account.
- Disclose a password in response to an unsolicited telephone call, message or email.

Approved password-management tools must be used where provided. Computers and other devices must be locked whenever they are left unattended.

Any suspected disclosure, loss or compromise of a password must be reported immediately to the ISMS Manager or the Director of Quality and Compliance. The affected password must be changed or disabled as soon as reasonably practicable.

User, Device and Network Accounts

Personnel must use individually assigned accounts wherever technically possible. Access must be authorised, limited to what is required for the person's role and reviewed in accordance with Crystal Health Group's access-control arrangements.

Generic or shared accounts must be avoided. Where a shared account is technically unavoidable, its use must be approved and documented. Access must be restricted to authorised personnel and the password must be changed whenever access requirements change, an authorised user leaves or a compromise is suspected.

Remote, wireless and network access must be provided only through authorised systems and appropriate security controls.

Client Case Authentication

Before discussing or disclosing information relating to a client case, personnel must verify the identity and authority of the person making the enquiry.

The preferred method is confirmation of the case reference and the case password or other authentication information established when the service was arranged.

Where the required information is unavailable, personnel must complete proportionate alternative verification using a sufficient combination of information already recorded on the case. This may include:

- The client's full name and date of birth.
- The telephone number or email address recorded on the case.
- The postal address recorded on the case.
- Relevant information about how the service was arranged or paid for.
- Other information known only to the client or an appropriately authorised person.

Only the minimum information necessary to establish identity and authority should be requested. If the responses do not provide sufficient confidence, no case information may be disclosed.

Any uncertainty or exception must be referred to the Director of Quality and Compliance or the Company Director. Authentication checks and any subsequent disclosure must be recorded in the relevant case record.

Third-Party Authority

Information may only be disclosed to a third party where their identity and authority have been established and documented.

Where the person making the enquiry is not the client or test participant, personnel must confirm whether they are:

- Acting under documented authority from the client or test participant.
- Acting for an employer, solicitor or other organisation that arranged the service under an appropriate contract or documented instruction.
- Otherwise legally entitled to receive the information.

Where suitable authority cannot be confirmed, no information may be disclosed. The client or test participant must provide the necessary authority before the enquiry can proceed.

Electronic Confidential Documents

Electronic documents containing personal data, special category data, test results, medical reports or other confidential information must be transmitted using an approved secure method.

Where password protection is used, the password must be communicated separately from the document it protects. The identity, authority and contact details of the recipient must be verified before the password is issued or reissued.

The approved password construction, issue timing, communication method and arrangements for private clients, SLA clients, authorised third parties, sample collectors, laboratories and other approved suppliers are controlled through **SOPCRY003Q – Document Control.**

Personnel must:

- Follow the current approved version of the Document Control SOP.
- Use only the password construction applicable to the relevant recipient or service type.

- Not create or adopt alternative password formats without authorisation.
- Follow the documented exception process where the usual communication method is unavailable.
- Report any suspected disclosure or compromise immediately.

Personnel who issue password-protected documents must receive appropriate training and be assessed as competent in accordance with the Document Control SOP.

External Users and Service Providers

Clients, sample collectors, laboratories, occupational health providers, suppliers and other authorised external users must be provided with individual or appropriately controlled access credentials wherever possible.

Access must be limited to the information and systems required for the agreed service. External users must notify Crystal Health Group promptly if their credentials are lost, disclosed or suspected of being compromised.

Third-party systems and applications must be protected using the security controls available within the relevant service, including strong passwords and multi-factor authentication where supported.

Password Reset and Account Recovery

Passwords may only be reset by the ISMS Manager, an appropriately authorised system administrator or the relevant approved service provider after the identity and authority of the requester have been verified.

Temporary passwords must be communicated securely and changed at first use where the system supports this. Access must be withdrawn promptly where it is no longer required.

Case Security Procedure

Before releasing case information, personnel must:

1. Identify the person making the enquiry and establish their relationship to the case.
2. Confirm that the person is the client, test participant or an appropriately authorised third party.
3. Verify the case reference and password or complete proportionate alternative identity checks.
4. Decline to disclose information if identity or authority cannot be established.
5. Escalate uncertain or exceptional cases to the Director of Quality and Compliance or the Company Director.
6. Disclose only the information the verified recipient is authorised to receive, using an approved secure communication method.
7. Record the identity checks, authority and disclosure in the relevant case record.

Requests made under data protection legislation, including subject access requests, must be managed under the Privacy Policy and the applicable data rights procedure. No routine administration charge may be applied to a statutory request except where permitted by law.

Any charge for a separate commercial service, such as an additional or replacement report, must be clearly distinguished and applied in accordance with the relevant terms of service.

4.4 Email, Internet and Software Use

Crystal Health Group provides email, internet access, networks, devices and software for authorised business purposes. Personnel are responsible for using these resources securely and appropriately.

Email Use
Only company-approved email accounts and services may be used to conduct Crystal Health Group business.

Email must be treated in the same way as any other form of written business communication. Content that would be unacceptable in a letter, document or face-to-face communication is equally unacceptable in an email.

Personnel must:

- Check recipients, attachments and content before sending an email.
- Use approved secure methods when sending personal, confidential or special category information.
- Follow the electronic document protection requirements in section 4.3 and SOPCRY003Q – Document Control.
- Remain alert to suspicious emails, links, attachments and requests for information or payment.
- Report suspected phishing, impersonation or email compromise immediately.
- Not automatically forward company email to a personal or unauthorised external account.
- Not send unlawful, discriminatory, abusive, offensive or inappropriate material.

Contracts, commitments and negotiations entered into by email must be treated as if they were entered into in writing and may only be undertaken by appropriately authorised personnel.

Company email accounts must be protected in accordance with the password and authentication requirements in section 4.3.

Where Crystal Health Group has reasonable grounds to suspect misuse, fraud, a security incident or another serious breach of company requirements, it reserves the right to access or monitor relevant company email communications. Any access or monitoring must be necessary, proportionate, appropriately authorised and undertaken in accordance with applicable law.

Administrative access to the company email system is restricted to the Company Director acting as ISMS Manager and any appropriately authorised technical service provider.

Internet and Wi-Fi Access
Company internet access must be used for authorised business purposes. Personnel must not use company systems to access, download, store or distribute unlawful, obscene, abusive, discriminatory or otherwise inappropriate material.

Accessing content or posting material that may damage the reputation of Crystal Health Group is prohibited and may result in disciplinary action.

Personnel must not attempt to bypass security controls or access restrictions.

Only authorised devices may connect to Crystal Health Group's corporate network. Personal devices must not connect to the corporate network unless their use has been specifically authorised.

Visitors, auditors, contractors, clients and other external persons must not connect their devices to the corporate network. They must use their own mobile data connection or personal hotspot unless a separately controlled guest connection has been made available.

Company devices must be protected by approved antivirus and security software and must receive applicable security updates.

Installation of Software
Only licensed software, applications and browser extensions approved by the ISMS Manager or an authorised technical provider may be installed or downloaded onto company devices.

Personnel must not install or use unauthorised software on Crystal Health Group systems.

4.5 ICT Fault Reporting

ICT faults affecting company computers, systems, applications, networks or communications must be reported promptly.

Where a fault cannot be resolved through the normal approved steps available to the user, it must be reported to the ISMS Manager. Personnel must not attempt unauthorised repairs, install software or alter system settings.

The ISMS Manager may deal with the fault directly, delegate the matter to an appropriate member of personnel or contact the relevant approved service provider for support.

The person who reported the fault must be kept informed of any relevant update and advised when the matter has been resolved.

Where an ICT fault involves or may involve:

- Unauthorised access.
- Malware or suspicious activity.
- Loss or disclosure of information.
- Compromised passwords or accounts.
- Loss of access to important information or systems.

It must also be treated as a potential information security incident and reported immediately to the ISMS Manager.

Where personal data may have been affected, the personal data breach requirements in section 4.2 must be followed.

4.6 Asset Register and Management

Crystal Health Group maintains an asset register of electronic devices owned and used by the company. This assists with the identification, allocation and management of company equipment.

For the purposes of this section, an asset is a company-owned electronic device used in the operation of the business. This includes:

- Desktop computers and laptops.
- Tablets and mobile telephones.
- Servers and network equipment.
- Printers and scanners.
- External drives and other electronic storage devices.
- Other relevant computer or communications equipment.

Each applicable asset must be allocated a numbered asset label and recorded in the asset register.

The asset register must include sufficient information to identify the equipment, the person or location to which it has been assigned and its current status. It must be updated when equipment is issued, reassigned or removed from use.

The ISMS Manager is responsible for maintaining the asset register. The current register is stored securely, with access restricted to the Company Director, Director of Operations and Director of Quality and Compliance.

Personnel issued with company equipment are responsible for taking reasonable care of it and must promptly report any loss, theft, damage or fault.

Reassignment and Disposal of Assets
Before an electronic asset is reassigned, sold, returned, recycled or disposed of, any company or personal information held on it must be securely removed. The device must be reset or securely erased as appropriate.

The asset register must be updated to record that the asset has been removed from use or reassigned. Where an asset is reused internally, its new user or location must be recorded.

No company asset may be sold, disposed of or removed from company premises without the approval of the ISMS Manager.

Where an asset cannot be securely erased internally, an approved specialist provider must be used. Disposal of any information or records held on the asset must also comply with the Archiving Policy.

4.7 ICT Equipment

Malware Protection
Company computers and other applicable devices must be protected by approved and licensed antivirus or security software.

Devices must not be connected to the corporate network unless the required security protection is installed and active. Any suspected virus, malware or other security concern

must be reported immediately to the ISMS Manager.

Personnel must not disable or interfere with antivirus software, security updates or other protection installed on company equipment.

Mobile Devices and External Storage
Only approved Crystal Health Group mobile telephones, tablets and laptops may be used to access company systems or information unless alternative arrangements have been authorised by the ISMS Manager.

External storage devices must not be connected to company computers or networks without prior authorisation. Where their use is authorised, they must be checked for viruses or malicious software before use.

Tablets Used by Sample Collectors
Tablets issued to sample collectors are provided solely to support authorised sample-collection duties.

Personal use is prohibited. Sample collectors must not access information or system functions outside the requirements of the authorised collection, including client records or test information unrelated to that collection.

Any misuse of a company tablet or unauthorised access to information may result in withdrawal of access and further action where appropriate.

Procurement of ICT Equipment
The purchase of ICT equipment, software or related services must be authorised by the ISMS Manager. This ensures that equipment and services are suitable for their intended purpose and compatible with existing company systems and security arrangements.

Removal of Equipment from Company Premises
Desktop computers, servers and other equipment intended to remain at Crystal Health Group premises must not be removed without permission from the ISMS Manager.

Company laptops, tablets and other portable devices may be removed for authorised business activities. Personnel are responsible for keeping such equipment secure while it is away from company premises and must promptly report any loss, theft or damage.

Disposal of ICT Equipment
ICT equipment and electronic storage media must be securely erased before they are reused, sold, recycled or disposed of.

4.8 ICT Access on Commencement and Exit

Commencement
The relevant Function Head Director must inform the ISMS Manager of the commencement date of a new employee and confirm the level of system access required for their role.

The ISMS Manager will arrange the required company email account, system access and equipment. Access must be limited to the systems and information needed for the employee’s role.

The employee must complete the applicable information security training and must not be given another person's login details or password.

Termination of Employment
The relevant Function Head Director must notify the ISMS Manager as early as reasonably possible of an employee's confirmed leaving date so that the removal of access can be arranged.

On or before the employee's final working day, as appropriate:

- Access to company email, systems, networks and remote services must be disabled.
- Company equipment, keys and other company property must be returned.
- Passwords for any shared accounts known to the employee must be changed where necessary.
- Access provided through external systems or service providers must be removed.
- Any applicable customer or supplier contacts must be informed of the employee's departure where operationally necessary.

Relevant business emails, calendars and files may be transferred to an authorised company location before the employee's account is deleted. An automatic email response or redirection to an appropriate company email address may be applied where necessary to maintain business continuity.

Information must only be retained where there is a legitimate business, contractual or legal requirement. Payroll, employment and other required records must be retained and subsequently disposed of in accordance with applicable legislation and the Archiving Policy.

Where employment ends unexpectedly or there is an identified security concern, access may be withdrawn immediately on the instruction of the Company Director or relevant Function Head Director.

4.9 Staff and Building Security

Crystal Health Group takes reasonable measures to protect its personnel, contractors, visitors, information and physical assets while they are on company premises.

Responsibility for the security of the building is shared between the landlord and Crystal Health Group. The Company Director and Director of Operations are responsible for the day-to-day management of the security arrangements within Crystal Health Group's offices.

Access and Responsibilities
Access to the main building and Crystal Health Group's offices is restricted to authorised persons using the relevant entry system, key or access code.

Personnel must:

- Keep keys, access codes and identification cards secure.
- Not share keys or access codes without authorisation.
- Challenge or report any suspicious or unauthorised activity.
- Ensure doors and other access points are secured when required.
- Follow the relevant fire, health and safety and emergency arrangements.

Security responsibilities and arrangements are communicated through induction, staff briefings and relevant training.

Personnel Access and Identification
Personnel are provided with the building and office access required for their role and, where applicable, an official identification card.

Personnel must sign in and out using the established office arrangements and display their identification card while on the premises.

Keys, identification cards and any other access devices must be returned when employment or engagement ends. System and physical access must be withdrawn in accordance with section 4.8.

Visitors and Contractors
Visitors and contractors must:

- Sign in and out using the visitors' book.
- Display the identification badge provided while on the premises.
- Remain accompanied by an authorised member of personnel unless alternative arrangements have been specifically approved.
- Follow all applicable security, health and safety and emergency instructions.

Contractors must check in and out each day with the Company Director, Director of Operations or a nominated member of personnel.

Personnel receiving a visitor or contractor are responsible for ensuring these requirements are followed.

Keys and Access Codes
Keys must only be issued to authorised personnel. The allocation of keys must be recorded in the company's asset or key register, and keys must not be lent, copied or transferred without authorisation.

Keys in circulation will be verified through the existing monthly safety spot-check arrangements.

Access codes must be kept confidential and changed where they are believed to have been disclosed or compromised.

Lost or Stolen Keys
Lost or stolen keys, identification cards or access devices must be reported immediately to the Company Director, Director of Operations or ISMS Manager.

The circumstances and potential security risk must be assessed so that appropriate action can be taken. This may include:

- Changing relevant access or alarm codes.
- Replacing affected locks where necessary.
- Informing relevant personnel.
- Reporting a theft to the police where appropriate.
- Recording the matter through the existing Quality Incident Reporting process where the loss presents a material security risk.

Keys must not be marked or stored with information that identifies the relevant premises or access point.

Failure to take reasonable care of keys or comply with these requirements may be addressed in accordance with the Staff Handbook and applicable disciplinary procedures.

Emergency Arrangements
Fire and evacuation arrangements are set out in the Fire Evacuation Policy. Other building emergencies, including theft, burglary or loss of access to the premises, are managed under the Business Continuity Plan.

This section should be read alongside the Staff Handbook, Health and Safety Policy and Business Continuity Plan.

4.10 Payment Card Security and PCI DSS Compliance

Crystal Health Group must protect payment card information and comply with the Payment Card Industry Data Security Standard (PCI DSS) requirements applicable to the payment methods and systems it uses.

Payments must only be processed through payment service providers and systems approved by Crystal Health Group. Payment card information must not be stored within Crystal Health Group's systems.

Handling Payment Card Information
Personnel handling payment card information must:

- Only use approved payment systems and processes.
- Treat payment card information as confidential.
- Ensure payment screens, terminals and documents cannot be viewed by unauthorised persons.
- Lock their computer or payment terminal whenever it is left unattended.
- Check that payment information is being entered into the correct approved system.
- Immediately report any suspected loss, disclosure, misuse or compromise of payment information.

Payment card information must not be:

- Recorded in emails, instant messages, case notes or other company documents.
- Written down or retained after the payment has been processed.
- Stored on company computers, mobile devices, shared drives or other local systems.
- Disclosed to an unauthorised person or third party.
- Copied into any system that has not been approved for processing payments.

The card security code, PIN or other sensitive authentication information must never be retained after authorisation.

Telephone Payments and Call Recording
Where payment card details are provided during a recorded telephone call, the call recording must be paused before the card details are given and resumed only after the payment information has been entered and the payment completed.

Payment card details must not be repeated aloud unnecessarily or included in any recorded call, voicemail or written communication.

Payment Service Providers
Only payment service providers approved by Crystal Health Group may be used.

Payment service providers must be subject to the company's supplier approval arrangements and must maintain appropriate payment security and PCI DSS compliance for the services they provide.

Access to payment systems must be restricted to authorised personnel and protected in accordance with the password and authentication requirements in section 4.3.

Compliance and Review
The Company Director, acting as ISMS Manager, is responsible for ensuring that Crystal Health Group completes any PCI DSS self-assessment, compliance confirmation or other validation required by its payment service provider or acquiring bank.

Technical vulnerability scans or other PCI DSS testing will only be undertaken where required for the company's payment environment and applicable method of compliance.

Any suspected compromise of payment card information must be reported immediately and managed through the Quality Incident Reporting process and, where personal data may have been affected, the personal data breach requirements in section 4.2.

4.11 Cloud Services, Configuration and Development

Crystal Health Group uses approved cloud-based systems and services to support its business activities, including systems such as Swiftcase and Daktela CRM.

Only cloud services approved by the Company Director, acting as ISMS Manager, may be used to store, access or process company information. Personal cloud-storage accounts must not be used for company information or business activities.

Cloud-service providers must be managed through the company's existing supplier approval and review arrangements. Consideration must be given to:

- The nature and sensitivity of the information being processed.
- The security and access controls provided.
- Data protection and confidentiality requirements.
- Data storage and backup arrangements.
- Service availability and business continuity.
- The provider's contractual and regulatory responsibilities.

Access to cloud services must be restricted to authorised users and protected in accordance with the password and authentication requirements in section 4.3. User access must be amended or removed when roles change or employment or engagement ends.

Where Crystal Health Group undertakes configuration, integration or development work, appropriate controls must be applied. These include:

- Restricting access to authorised personnel or approved service providers.
- Testing significant changes before they are introduced into live use.

- Obtaining appropriate approval before changes are implemented.
- Avoiding the use of live personal or confidential information for testing unless its use has been specifically authorised and adequately protected.
- Maintaining a record of significant changes through the existing supplier, document-control or quality-management arrangements, as applicable.

Any suspected compromise, unauthorised access or loss of information involving a cloud service must be reported immediately and managed under the relevant incident and personal data breach arrangements in this policy.

4.12 Use of Artificial Intelligence Tools

Crystal Health Group recognises that artificial intelligence (AI) tools, including ChatGPT and similar platforms, may support appropriate business activities such as research, drafting and process improvement.

AI tools may only be used by authorised personnel, through platforms approved by the Company Director, and in accordance with this Information Security Policy.

Permitted Use
Approved AI tools may be used for:

- General business research and information gathering.
- Drafting or improving non-sensitive content.
- Generating ideas to support business processes and efficiency.
- Summarising or reviewing information that does not contain personal, confidential or commercially sensitive information.
- Supporting analysis where the information provided has been fully anonymised.

Information produced by an AI tool must be reviewed and verified by an authorised person before it is relied upon, published, communicated externally or used to support a business decision.

Prohibited Information
Personnel must not enter, upload or process any of the following within an AI tool:

- Personal data relating to an employee, client or third party.
- Special category data, including health, medical or genetic information.
- Client-specific information or identifiable case details.
- Confidential or commercially sensitive business information.
- Passwords, access credentials or security information.
- Payment card information.
- Information subject to contractual, legal or regulatory restrictions.

Removing a person’s name may not be sufficient to anonymise information. Details must not be entered where an individual, client, organisation or case could still be identified directly or indirectly.

Generic descriptions such as “employee”, “client” or “individual” may be used only where they cannot be connected with an identifiable person, organisation or case.

Business Decisions and External Communications
AI tools must not be used to:

- Make decisions about individuals without appropriate human review and oversight.
- Issue communications to clients or third parties without review by an authorised person.
- Store official company records or act as the company's system of record.
- Replace professional, legal, clinical or regulatory advice.
- Produce or approve contractual, legal or regulated content without appropriate review.
- Circumvent any company approval, quality-control or document-control requirement.

Personnel remain responsible for checking the accuracy, suitability and originality of AI-generated content and for identifying any misleading, biased, incomplete or unsupported information.

Data Handling and Incidents
If personal, confidential or otherwise restricted information is entered into an AI tool inadvertently:

- No further information must be entered.
- The content or conversation must be deleted where this is possible.
- The incident must be reported immediately to the ISMS Manager.
- The information security incident and personal data breach arrangements in section 4.2 must be followed where applicable.

Any business content produced with the assistance of AI that is required as an official record must be transferred to the appropriate approved company system and managed under the normal document-control and retention arrangements.

AI tools must not be used as ongoing storage for company information. Business-related prompts, conversations and generated content should be removed when they are no longer required.

Responsibility
Authorised users are responsible for ensuring that their use of AI tools complies with this policy and all applicable confidentiality, data protection, information security and intellectual-property requirements.

Failure to comply with this section may result in disciplinary action in accordance with company procedures.

5. Version Control

Previous Version	Changes	Last Effective Date	Reviewed and authorised by:
v10.01.26	Full annual review and transfer into the approved Word policy template. Policy structure simplified and sections renumbered. Responsibilities and job titles updated. Information security controls reviewed and updated, including personal data breaches, passwords and authentication, email and internet use, ICT faults, asset and equipment management, personnel access, building security, payment card security, cloud services and use of AI tools.	18/08/2026	John McChrystal
v09.09.25	Addition of Section 5.12 – Use of Artificial Intelligence (AI) Tools	07/01/2026	John McChrystal
v09.09.24	• Addition of 3.1 Information Security Roles and Responsibilities • Updated Clause 2.1 to reference ISO/IEC 27001:2022 and Annex A (Organisational, People, Physical, Technological) • Section 5.4: Added restrictions on WiFi access for staff and visitors • Section 5.7: Clarified sample collector tablet use policy • Section 5.11: Added new section on secure cloud services and secure development • Added Section 5.12 – Threat Intelligence	10/09/2025	John McChrystal
v07.09.24	• Section 2.2 - Addition of Waste Electrical and Electronic Equipment (WEEE) regulations • Section 5.9 - Addition of Policy for Lost or Stolen Keys	17/12/2024	John McChrystal
v06.08.24	• Section 5.1 - Addition of reference to Statement of Applicability document. • Section 5.3 - Update to Sample Collection Network Password	20/09/2024	John McChrystal

	• Section 5.7 - Addition of Only approved Crystal Health Group assets • Addition of third party supplier in the disposal of ICT assets.		
v05.06.23	• Section 5.3 - Update to employee responsibility regarding 'Third Party Vendor Systems & Applications' section. • Section 5.10 - Addition of call recording to PCI compliance section.	23/08/2023	John McChrystal
v04.06.21	• Section 5.3 - Password creation guidance and employee responsibility for password protecting access to their PC. • Case security – removal of £10 charge for third party consent form. However, this must be considered if this is requested after an appointment – see note at the bottom of page 10. • Section 5.4 - Employee responsibility for password protecting Gmail account.	13/06/2023	John McChrystal
v03.03.20	• Addition of Section 5.10 'PCI Compliance'	02/06/2021	John McChrystal
v02.04.18	• Update to Section 5.3 - Password Protection. Sub-section 'Electronic Documents Passwords'	11/03/2020	John McChrystal
v01.07.17	• Review and update to format of policy. • Addition of GDPR and associated procedures. • Consolidation of smaller ICT policies into this policy.	04/04/2018	John McChrystal