Crystal Health Group

Information Security Policy

Contents

1. Purpose

Crystal Health Group Limited recognises that individuals and organisations with which we conduct business, value their privacy. In order to provide timely and secure services, the collection of client information is necessary to fulfil the contract of service. Crystal Health Group Limited is committed to protecting the privacy and security of individual and commercial clients whilst conducting its business, specifically related to the provision of DNA, drug and alcohol testing and Occupational Health services.

It is our intent to prevent and minimise the impact of information security incidents and deliver assurances to clients and other stakeholders that its information assets are protected from all types of threat, whether internal or external, deliberate or accidental.

2. Scope

The Director John McChrystal is ultimately responsible for defining information security policy and standards. Other Directors, Managers and Staff are responsible for implementing the information security policies and standards. All employees and service providers of Crystal Health Group Limited are responsible for meeting the requirements of the policies and standards.

2.1 ISO/IEC 27001:2022, including Annex A (Organisational, People, Physical, and Technological controls)
ISO/IEC 27001:2022 will be the primary reference for designing and implementing information security within Crystal Health Group Limited. The use of the Standard will enable Crystal Health Group Limited to deploy security controls consistently across all business units and to define its requirements for security in all third party contracts and partnerships. The Standard also provides a means of benchmarking against other organisations and a method of checking that security polices and standards are being implemented effectively.

On review, the Crystal Health Group Limited strategic direction for information security has established an effective, forward-looking management system, clearly aligned with the company’s commercial direction and supported by a strong professional and technical capability across the organisation.

Crystal Health Group Limited is able to demonstrate that clients, business partners, employees and agents can have full confidence in the confidentiality, integrity and availability of our information services and IT infrastructure through our ISO/IEC 27001:2022 ISMS procedures and associated records.

2.2 Applicable Legislation

- General Data Protection Regulation May 2018
- The Computer Misuse Act 1990
- The Privacy and Electronic Communications (EC Directive) Regulations 2015
- The Telecommunications Regulations 2000
- Waste Electrical and Electronic Equipment (WEEE) regulations

To view the above documents, please visit: http://www.legislation.gov.uk/browse

3. Responsible Person(s)

The Policy Author is responsible for:

- Accuracy, version control and review dates.
- Implementation, training and operational compliance of this Policy.
- Initiating Policy change requests.

The QA representative is responsible for:

- Ensuring adherence to company Policy standards for authoring, content and structure.
- Resolution of Quality Incident reports arising from noncompliance of this Policy or external complaints.

Trained personnel are responsible for complying with all aspects of this Policy.

3.1 Information Security Roles and Responsibilities

Crystal Health Group assigns clear responsibilities for the implementation and ongoing management of its Information Security Management System (ISMS). These responsibilities are defined to ensure compliance with ISO/IEC 27001:2022 and to maintain the confidentiality, integrity, and availability of client and company data.

Responsibility Area	**Responsible Person(s)**
Overall ISMS management and accountability	Director – John McChrystal
Access provisioning and termination	Director / Operations Manager
Device assignment and recovery	Operations Manager / Business Development Manager
Incident reporting and escalation	All staff / QA Manager
Policy review and approval	Director and Management Team
Supplier due diligence and assurance	Quality Manager

These responsibilities are communicated to staff during induction and annual refresher training. Subcontractors are issued with relevant security policies and updated via secure access or email as required.

4. Health & Safety

All tasks and activities associated with this Policy comply with Crystal Health Group's Health & Safety Policy.

THIS SPACE LEFT INTENTIONALLY BLANK

5.1 Data Protection

Crystal Health Group is required to comply with the General Data Protection Regulation (GDPR) requirements that came into force in May 2018.

Crystal Health Group is registered under the Data Protection Register with the Information Commissioner's Office (ICO), Registration No. ZA260675.

Our Client Privacy Policy details the provisions in place to comply with GDPR and provides transparency and guidance to our clients with regards to their rights to how their personal data is processed and retained. The current version of the policy can be viewed at: https://www.crystal-health.co.uk/privacy-policy/

We use approved third party vendor systems to enable electronic order processing, including appointment coordination, order tracking, results reporting and financial control. Information security controls for all electronic systems is detailed in our current ISO/IEC 27001:2022 Statement of Applicability document.

5.2 Personal Data

Due to the nature and sensitivity of the personal data Crystal Health Group processes, it is vital that we have robust breach detection, investigation and internal reporting procedures in place.

The investigation and internal reporting of personal data breaches is processed through the existing Quality Incident Reporting (QIR) system. This ensures that all data breaches are recorded for future reference.

This section of the information security policy details the following processes and procedures:
- Identifying a personal data breach.
- Our response plan for addressing any personal data breaches that occur.
- The team responsible for managing breaches and escalation process.
- The process to assess the likely risk to individuals as a result of a breach.
- The relevant supervisory authority for our processing activities.
- The process to notify the ICO of a breach.
- The process to inform affected individuals about a breach.
- What information about a breach we must provide to individuals.

What is a personal data breach?
A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed.

Personal data breaches can include:
- Access by an unauthorised third party;
- Deliberate or accidental action (or inaction) by a controller or processor;
- sending personal data to an incorrect recipient;
- computing devices containing personal data being lost or stolen;
- Alteration of personal data without permission; and
- Loss of availability of personal data.
- The above also includes any data processors used by Crystal Health Group who process personal data on behalf of the company.

If any of the above incidents occur, you must inform the Quality and Compliance team immediately. Do not attempt to resolve the matter yourself, as a robust assessment of the incident and appropriate follow-up actions must be performed by the relevant manger within this team. See Responsibility and Escalation section below.

Response plan

Further to the above, a consistent approach is required to ensure data breaches are thoroughly investigated by authorised personnel. The following actions must be followed for all cases of a data breach:

1. **Identify the personal data breach.**
2. **If we receive notification of a data breach. Inform the individual to detail in writing the nature of the breach and all other relevant details via email to info@crystal-health.co.uk and for the attention of the Quality and Compliance team. Alternatively, provide the current postal address for Crystal Health Group head office for the individual to send by post.**
3. **An acknowledgement must be provided to any notification of a data breach in accordance with Crystal Health Group's Complaint Handling policy.**
4. **Pass all details of the breach to the Quality and Compliance team.**
5. **The Quality and Compliance team will assess the severity of the data breach and determine the effects on the individual(s) and if the ICO must be notified. See following sections for further details.**
6. **If applicable, the ICO will be notified of the data breach. This must be done within 3 working days of becoming aware of the data breach. See following sections for further details.**
7. **Based on the severity of the data breach and the output from the risk assessment performed, the individual(s) affected must be informed as soon as possible. See following sections for further details.**
8. **A QIR must be generated for all data breaches regardless of point 5. Refer to Crystal Health Group SOP 'Quality Incident Reporting'.**
9. **The QIR will record and track all information with regards to the details, investigation, notes and reporting relevant to the data breach. The QIR reference must be used on all correspondence.**
10. **The Quality and Compliance team are responsible for the conclusion of the investigation. This includes reporting all findings, preventative measures and working with the ICO if applicable on any follow-up actions.**
11. **On conclusion of the investigation, all interested parties will receive a report of the findings.**

Responsibility and Escalation

All data breach incidents will be reported to the Quality and Compliance team based at Crystal Health Group's head office. This team is responsible for the investigation and conclusion of the data breach, in accordance with the Response Plan set out in this policy. On occasion, it may also be necessary for staff to escalate the decision on whether or not a data breach has occurred to the Quality and Compliance team. Further escalation measures for serious data breaches are in place to the Company Director if required.

Risk Assessment of data breaches

When a personal data breach has occurred, we need to establish the likelihood and severity of the resulting risk to people's rights and freedoms.

In assessing risk to rights and freedoms, it's important to focus on the potential negative consequences for individuals.

This means that a breach can have a range of adverse effects on individuals, which include emotional distress, and physical and material damage. Some personal data breaches will not lead to risks beyond possible inconvenience to those who need the data to do their job. Other breaches can significantly affect individuals whose personal data has been compromised. We will assess this case by case, looking at all relevant factors.

Crystal Health Group utilise the risk assessment methodology as set out in the **'Recommendations for a methodology of the assessment of severity of personal data breaches'** document by the European Union Agency for Network and Information Security.

This working document is used on a case by case basis and considered a controlled document within the Quality Assurance and Compliance team. As such, updated versions of the document are regularly checked for at https://www.enisa.europa.eu/publications/dbn-severity

From this risk assessment methodology, the overall severity of the data breach can be determined. The score can then be classified as follows:

SE < 2	Low	Individuals either will not be affected or may encounter a few inconveniences, which they will overcome without any problem (time spent re-entering information, annoyances, irritations, etc.).
2 ≤ SE < 3	Medium	Individuals may encounter significant inconveniences, which they will be able to overcome despite a few difficulties (extra costs, denial of access to business services, fear, lack of understanding, stress, minor physical ailments, etc.).
3 ≤ SE< 4	High	Individuals may encounter significant consequences, which they should be able to overcome albeit with serious difficulties (misappropriation of funds, blacklisting by banks, property damage, loss of employment, subpoena, worsening of health, etc.).
4 ≤ SE	Very High	Individuals may encounter significant, or even irreversible, consequences, which they may not overcome (financial distress such as substantial debt or inability to work, long-term psychological or physical ailments, death, etc.).

Depending on the nature of the data breach, either the Quality Assurance Manager will perform the risk assessment and/or seek the assistance of the Compliance Manager. If required, Director input may also be requested. The output from the risk assessment will determine subsequent actions with regards to communicating the data breach to the ICO and individuals affected.

Regulatory Authority
Crystal Health Group comply with all requirements set out in the Human Tissue Act 2004. The Human Tissue Authority was created to regulate the Human Tissue Act. This governs the collection of biological samples for the purpose of all Crystal Health Group testing activities.

The Information Commissioner's Office (ICO) upholds information rights in the public interest, promoting openness by public bodies and **data privacy for individuals**. Crystal Health Group aim to comply with all requirements of the General Data Protection Regulation and is registered under the Data Protection Regulations 2018 No. ZA260675.

Notifying the ICO of a data breach
Depending on the outcome of the risk assessment, the ICO must be informed of a data breach within 3 working days of the data breach occurring.

Reporting a personal data breach to the ICO will be part of the overall internal QIR process. As such, personal data breaches will be reported using the on-line reporting form. This can be found at: https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/

The form will be downloaded and the initial report must be completed and returned within the 3 working day timescale. Instructions on how to return the form are detailed within the form itself.

The process to inform affected individuals about a breach
If a breach is likely to result in a high risk to the rights and freedoms of individuals, the GDPR says we must inform those concerned directly and without undue delay. In other words, this should take place as soon as possible.

There are two ways in which a personal data breach can be reported, these are:

1. An individual/organisation reports the personal data breach to Crystal Health Group.
2. The personal data breach is detected internally by a member of staff or contractor within Crystal Health Group.

In the case of the first method of reporting, the following response must be sent within 1 day of receiving the notification:

Thank you for contacting Crystal Health Group. We treat all reported personal data breaches seriously. Our Quality Assurance team will review the information you have provided and initiate an investigation. We will provide you with an initial update of our findings within 3 working days. In the meantime, we may need to contact you if we require any further information regarding the information you have provided.

The following process then applies regardless of the detection method:

1. **A risk assessment will be performed by the QA team - see 'Risk Assessment of Data Breaches'**
2. **The severity output of the risk assessment will determine the communication methods to the ICO and individuals affected by the breach.**
3. **If applicable the QA team with report the personal data breach to the ICO - see 'Notifying the ICO of a Data Breach'**
4. **If applicable, the QA team will write to the individuals affected, providing an initial report of the findings, the contact person performing the investigation and the likely time scales for completion and conclusion of the investigation. In addition, you need to describe, in clear and plain language, the nature of the personal data breach and, at least:**
   > a description of the likely consequences of the personal data breach; and
   > a description of the measures taken, or proposed to be taken, to deal with the personal data breach and including, where appropriate, of the measures taken to mitigate any possible adverse effects.

   Please note, any correspondence to individuals must be sent by their chosen method of communication. In all cases, responses must be in writing.

5. **The ICO and individuals affected by the breach must be kept updated with regards to the progress and eventual conclusion of the investigation.**

5.3 Password Protection

Password Generation
In line with information security best practice, the following password generation method must be used for Crystal Health Group's system applications and operating systems:

- Must contain at least one capital letter
- Must contain at least one lower case letter
- Must contain at least 1 number
- Must be at least 12 characters long
- We advise that passwords are made up using a 'pass phrase' consisting of 3 uncommon words

Computer Passwords
All Crystal Health Group's computer users are responsible for password protection for their workstation PC i.e. access to the Windows Operating System. Users must not disclose their passwords to another member of staff or any other person with exception to the IMS Manager. If a user forgets this password, they must inform the IMS Manager as soon as possible to arrange for the computer to be unlocked and the password reset. Refer to section 5.4 for email password protection.

Network Passwords
Crystal Health Group's shared network drive is a peer to peer Windows network. Initial authorised access to the shared network drive is granted by the IMS Manager using the 'Shared User' network password. The network is cabled meaning that no WIFI access is available.

Client Case Passwords
All DNA and Hair Tests performed by Crystal Health Group require a password that has been assigned by the client. All discussions regarding the test can only proceed if this is provided if the following information is provided.

- Case Password (if assigned)
- Case Reference number

Please refer to the diagram (process flow) **CASE SECURITY** on the next page if the above information cannot be obtained. If necessary, locate the case file using the information provided and ensure the details obtained are correct.

The above also applies to any authorised third parties.

Other test types do not require a client case password but do require confirmation of personal details, refer to the diagram on the next page for guidance.

The process diagram illustrates the procedure for obtaining the correct answers to security questions before disclosing any test case information.

Electronic documents Passwords
Any documentation that contains personal information (refer to Client Privacy policy) that can identify an individual must be password protected when sending by email. The following procedures are in place for electronic document password protection:

<u>DNA self-collection kits</u>

- The Swiftcase system is used to send the client an SMS text message with a password in the following format:

  cry-stAL@-XXXX where XXXX is the sequential number from the case reference number.

- For appointment based tests, the SMS text message will be sent at the case creation stage.
- For self-collection based tests, the SMS text message will be sent at the sample receipt stage.

- For authorised third parties, the SMS text message will be sent at the test result stage, unless otherwise requested.

All private clients and order confirmation clients

- The Swiftcase system is used to send the client an SMS text message with a password in the following format:

cry-stAL@-XXXX where XXXX is the sequential number from the case reference number.

- For appointment based tests, the SMS text message will be sent at the case creation stage.
- For self-collection based tests, the SMS text message will be sent at the sample receipt stage.
- For authorised third parties, the SMS text message will be sent at the test result stage, unless otherwise requested

SLA Clients

- All SLA clients will receive communication via secure email informing them of their unique password. This will be in the following format:

cry-stAL@-XXXX where XXXX is the SLA clients' 6 digit prefix from their own unique reference.

Sample Collection Network

- All sample collectors will receive communication via secure SMS informing them of their unique sample collection network password. This will be in the following format:
- **cry-stAL@-XXX** where XXX is the prefix used for sample collectors only.

Major suppliers, including laboratory partners

- Will receive communication via secure email informing them of their unique password. This will be in the following format:
- **cry-stAL@-XXX** where XXX is a number set by Crystal Health Group.

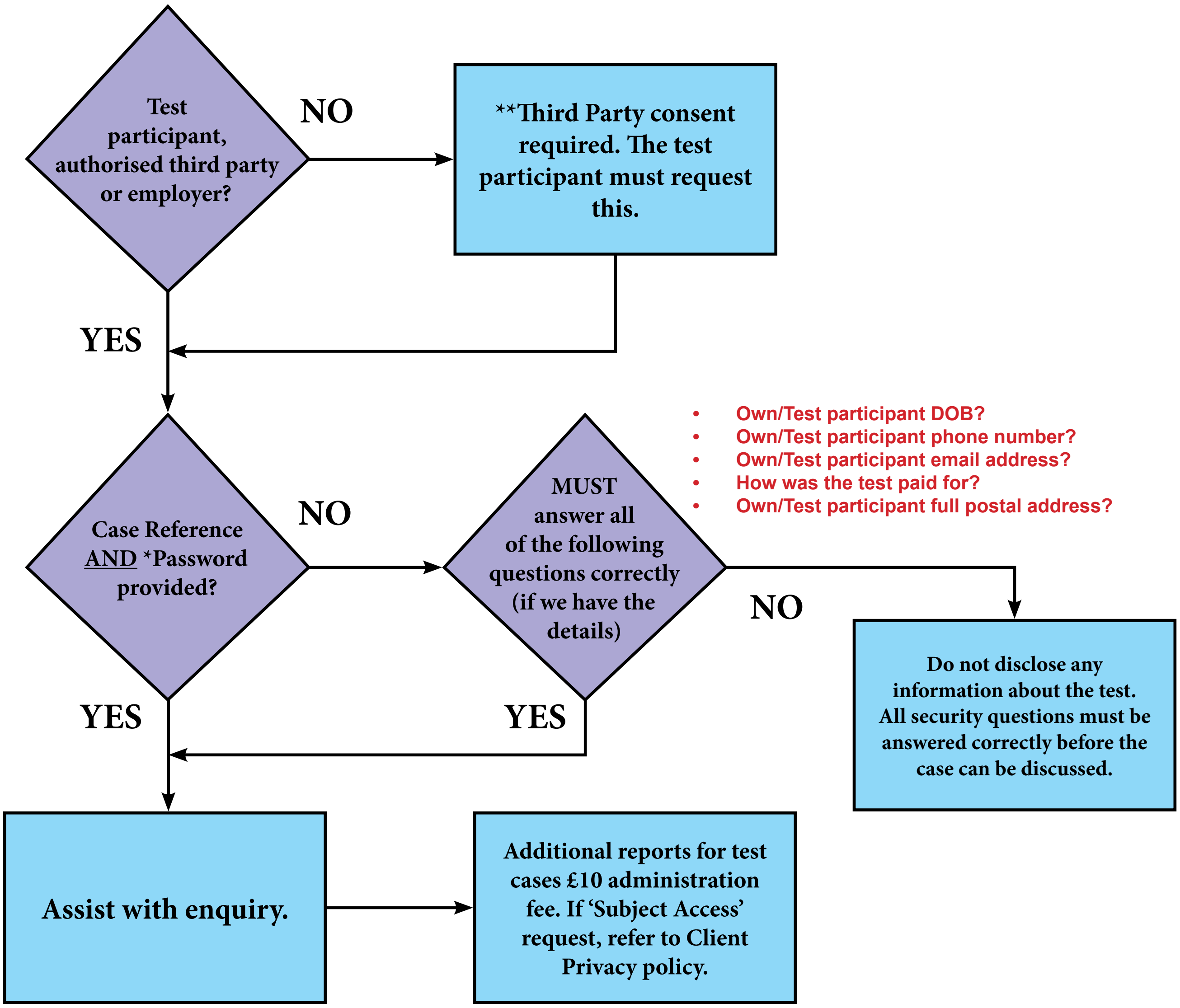
IMPORTANT
For those instances when a client does not have a mobile number to receive an SMS text message, we will resolve this on a case by case basis. The standard response would be to provide the password to the email address provided by the client. We must also inform the client to record the password and keep this in a safe place.

NOTE
The above processes are currently being implemented over time. Until fully implemented, the existing method of notifying clients of their password will continue by use of a second secure email.

Third Party Vendor Systems & Applications
All third party vendor systems & applications, including social media accounts, are password protected. Passwords for relevant systems are the responsibility of each member of staff and must follow password generation rules. If a password is forgotten or require a rest, the IMS Manager or authorised staff member will arrange for a password reset from the relevant vendor as soon as possible.

Case Security

The process diagram illustrates the procedure for obtaining the correct answers to security questions before disclosing any test case information.


Test participant, authorised third party or employer?
NO
**Third Party consent required. The test participant must request this.
YES
Case Reference AND *Password provided?
NO
MUST answer all of the following questions correctly (if we have the details)
- Own/Test participant DOB?
- Own/Test participant phone number?
- Own/Test participant email address?
- How was the test paid for?
- Own/Test participant full postal address?
NO
Do not disclose any information about the test. All security questions must be answered correctly before the case can be discussed.
YES
YES
Assist with enquiry.
Additional reports for test cases £10 administration fee. If 'Subject Access' request, refer to Client Privacy policy.

*** DNA and Hair Tests only.**

**** If a 'Third Party' form is required to be sent, then a £10 administration should be considered. This will generally only be the case if an appointment based collection has taken place and the client failed to mention a third party. Or, for a self-collecition DNA kit, when there is no option to add a third party as they are for personal information only.**

5.4 Email & Internet Access

Crystal Health Group use the Google email server service (Gmail). This system has integral anti-virus software installed. Each Crystal Health Group employee uses Microsoft Outlook to retrieve emails from the Gmail service. Employees are responsible for generating and regularly updating the gmail password following guidance from section 5.3. Password reset is managed by the IMS Manager John McChrystal. Each Crystal Health Group computer is installed with licensed Bit Defender anti-virus software.

Email should be treated like any other form of written communication and, as such, what is normally regarded as unacceptable in a letter or memorandum is equally unacceptable in an email communication. Contracts and negotiation entered to by e-mail must be treated as if entered into in writing.

Where Crystal Health Group have reasonable grounds to suspect misuse of email in either scale of use, content or nature of messages, it reserves the right to monitor the destination, source and content of email to and from a particular address.

The IMS Manager (John McChrystal) has full administration rights for email access and monitoring.

Internet and WiFi Access Access
Ethernet Internet access is provided to be used in the course of Crystal Health Group's business. Personal use is not allowed at any time in particular access to sites containing obscene, abusive or racist content.

Access to any site or the posting of material that may bring Crystal Health Group into disrepute is also strictly prohibited and may result in disciplinary action.

External visitors (including auditors, contractors, and clients) are strictly prohibited from connecting to Crystal Health Group WiFi. Visitors must use their own mobile data or personal hotspot. Internal staff must not connect personal devices to company WiFi under any circumstances. This restriction is in place to maintain information security and prevent unauthorised device access to the corporate network.

Installation of Software
Only licensed software approved by Crystal Health Group IMS Manager may be installed / downloaded on Crystal Health Group's computers.

5.5 Fault Logging (ICT)

This section defines the Policy of the logging, control and management of all ICT faults identified throughout the operation of Crystal Health Group's processes and computer systems to ensure that such faults are known, controlled and resolved.

We aim to ensure that all faults identified by a member of staff, not rectifiable in-house, are communicated to the IMS Manager (John McChrystal), who in turn will communicate and liaise with the relevant third party vendor for resolution.

The IMS Manager may deal directly with the third party vendor depending on the severity of the issue, otherwise the fault will be delegated to a nominated member of staff to conclude to resolution.

All third party faults are reported to vendors either by email or through dedicated help desk functions.

Updates on the fault and final resolution are communicated via email to the IMS Manager.

The IMS Manager will communicate to individuals/team final resolution and any preventative control measures required for future occurrences.

5.6 Asset Register & Management

As part of Crystal Health Group's Information Security Management system, we identified the need to implement, update and mange a register of electronic device assets owned by the company.

Electronic asset management has been designed to assist Crystal Health Group's management and employees with the labelling and registering of assets and the on-going maintenance of the asset register.

What is an asset?
An asset can be defined as anything that Crystal Health Group owns and uses within its function as a business. The scope of this policy covers electronic device assets owned by the company only.

What is an asset register?
The Crystal Health Group asset inventory is an inventory held of all logged electronic asset devices. These items are mainly computing related devices owned, managed and used within the company. These devices include computers (desktops, notebooks, servers), network devices (switches, routers, etc), printers, appliances (flash drive storage, cameras, etc).

Each item is labelled with an approved, numbered asset label and logged into the asset register. The IMS Manager (John McChrystal) is responsible for the asset labelling and logging. The asset register is controlled by the IMS Manager who takes the responsibility for its maintenance as an integral element of Information Security requirements.

Where is the information logged?
The most recent copy of the asset register is located on the Dropbox Server. Access to the register is restricted, encrypted by password protection and is available only to the IMS Manager, Operations Manager, and Quality Manager.

Disposal of assets
All assets must undergo a cleansing process – information must be wiped, a system reset operated, prior to storing the out of life asset. All end of life assets must be noted on the asset register, an 'out of use' label applied to the asset and the unit stored in the assigned storage area. If you are unsure where this is, please ask your line manager.

No asset should be sold or removed from the property without the express permission of the IMS Manager.

5.7 ICT Equipment

All IT equipment provided for employee use is intended primarily to be used in the conduct of Crystal Health Group's business. Personal use of ICT equipment is prohibited unless written authorisation is granted by the Information Security Manager John McChrystal.

Under no circumstance must Crystal Health Group's ICT facilities be used in a way likely to harm or disrupt Crystal Health Group's business.

Anti Virus Protection
All PC's and other devices must be checked by the IMS Manager to ensure they are free from any virus or malicious software prior to connection with Crystal Health Group's network.

All workstations and servers must be installed with the approved and licensed Bit Defender anti-virus or other software approved by the IMS Manager prior to connection to the network.

No computer will be connected to the network unless it complies with these protection criteria.

Mobile devices

This includes:

- Mobile phones - Only approved Crystal Health Group assets
- External storage devices - Crystal Health Group prohibit the connection of all external storage devices to all PC's and network without prior authorisation and virus scanning from the IMS Manager.
- Tablets - Only approved Crystal Health Group assets
- Laptops - Only approved Crystal Health Group assets

Tablet Use by Sample Collectors

Tablets issued to sample collectors are for the sole purpose of supporting active sample collection duties. Use of these devices for personal purposes is strictly prohibited. Accessing data or system features outside the scope of an authorised collection (including client records post-collection, test results, or other users' details) is considered a breach of this policy and may result in disciplinary action. All activity on tablets is logged and subject to audit.

Procurement of ICT Equipment

All procurement of ICT equipment or services must be authorised in writing by the IMS Manager.

Removal of Equipment from Crystal Health Group's Premises

Desktop computers and servers must not be removed from Crystal Health Group's premises without permission from the IMS Manager. Only approved Crystal Health Group assets can be removed from the premises for authorised tasks.

Disposal of ICT Equipment

When disposing of any ICT equipment, all hard drives and removable data storage media must be securely deleted. The disk must be rendered unusable in a manner to prevent a 3rd party from accessing the original files and data. This is undertaken by an approved supplier with the hardware disposed of in a sustainable manner. All associated documents will be secured in locked cabinets when not in use. Unwanted documents will be shredded. Refer to section 5.6 Asset Register and Management for detailed instructions.

5.8 ICT Staff Registration & Exit

Commencement

The relevant Director/Manager will contact the IMS Manager in order to confirm the commencement date of the new employee and determine / confirm the level of system access required.

Termination

On termination of employment, all details relating to the person leaving will be deleted from all Crystal Health Group's operating systems to include email and internet access. The only exception for the retention of employee details will be payroll (third party vendor controlled), as per legislation.

All keys and will be returned in line with the Staff and Buildings Security in section 5.9 of this policy.

The IMS Manager will be contacted in advance of any predicted exit date and the deletion scheduled.

Customers will be contacted in order to provide prior notice of the departure of a staff member and where necessary request that all remote access for the person leaving be deleted from our customers' systems (if applicable).

Standard Process

- Disable access / change the password of primary systems on the email server and shared network server to prevent access.
- Extract sent / received emails to a secure reference facility; enabling access either from one of the shared folders on the network or on a local machine.
- Once calendar and emails have been extracted, delete the user account on the server.
- Set-up an email auto response on gmail diverting any emails to info@crystal-health.co.uk

5.9 Staff and Buildings Security

Commencement
Crystal Health Group's Directors are aware of the importance of maintaining a high level of personal security for staff, contractors and all visitors to the Head Office based in Manchester.

We have set out the measures that will be adopted to ensure, so far as is reasonably practical, that employees, contractors and all visitors are protected from risks to their Health and Safety.

Organisation
Responsibility for Building Security is shared between the Landlord and Crystal Health Group Directors. The identified individuals for day-to-day responsibility for Crystal Health Group's office security are as follows:

Security Access to Crystal Health Group's office:
John McChrystal and management

Control of Visitors to Crystal Health Group's office:
All Crystal Health Group's Staff

Control of Contractors to Crystal Health Group's office:
All Crystal Health Group's Staff

Emergency Procedures:
Fire: Designated Crystal Health Group's Fire Wardens
First Aid: Designated Crystal Health Group's First Aiders
Business Continuity Plan: As per current Policy

Information and Communication
Procedures and arrangements for security are detailed and regularly updated in:

- The Staff Handbook
- The Business Continuity Plan Policy
- Crystal Health Group's Health & Safety Policy

Security matters are addressed in:

- Induction Training for all new staff
- Regular updates as necessary during staff briefs and training
- Specific training on new equipment and systems as required

Visitors & Contractors
All visitors and contractors are required to sign in and out of Crystal Health Group office by completing the visitors book.

Visitors and contractors will be provided with an identification badge. This badge must be displayed at all times whilst they remain on the premises. All visitors and contractors must be accompanied at all times by a Crystal Health Group's member of staff whilst on the premises.

All contractors are required to check in and out each day with a Director or nominated deputy and comply with all other Crystal Health Group management controls.

General Access and Egress
Access to the main building is controlled by authorised entry only. Key management and personnel have access to the building keys to allow entry when required.

Access to the Crystal Health Group's office on the first floor can be accessed by key code entry only.

Policy for Lost or Stolen Keys

Reporting

Key holders must report lost or stolen keys to management immediately upon discovery, but no later than 24 hours. Prompt reporting is crucial to mitigate security risks. A written report detailing the incident must also be submitted.

Lost Keys

1. Risk Assessment:
    - Management will perform a risk assessment to determine the security implications and whether locks should be replaced.

2. Responsibility for Costs:
    - Key holders are responsible for the cost of replacing lost keys.
    - If management determines that replacing locks is necessary, the company will cover the cost of the replacement.

3. Security Measures:
    - The security alarm code must be updated immediately to prevent unauthorised access.
    - Management will ensure that all affected parties are informed of any changes to alarm codes or lock replacements.

4. Prevention:
    - Key holders are advised to take precautions to prevent loss, such as avoiding leaving keys unattended or attaching them to items with identifying information.

Stolen Keys

1. Investigation and Reporting:
    - Management will investigate the circumstances surrounding the theft.
    - If warranted, the theft will be reported to the police to ensure proper action is taken.

2. Replacement of Locks:
    - As a precaution, all locks associated with the stolen keys will be replaced to prevent unauthorised access.
    - The company will cover the cost of replacing the locks in the event of theft.

3. Security Code Update:
    - The security alarm code must be updated immediately.
    - Management will ensure affected staff are informed of the new codes to avoid disruptions.

4. Accountability:
    - Key holders may bear partial or full responsibility for costs if negligence is determined to have contributed to the loss or theft.

Key Circulation and Responsibility

- Key holders are listed on the companies asset register.
- Lending or borrowing keys is strictly prohibited. Each key is assigned to a registered key holder, who remains solely responsible for its safekeeping.
- During the monthly safety spot check, management will review and verify all keys in circulation to ensure compliance with the key management policy.

Documentation

- All incidents of lost or stolen keys must be documented using the QIR process, including a written report by the key holder and any actions taken by management.

Proactive Measures

To prevent future incidents, key holders should:

- Avoid leaving keys in visible or unsecured locations.

- Report any suspicious activity related to security promptly.
- Keep keys separate from items that may identify the owner or their workplace.

Accountability
Failure to adhere to this policy, including unauthorised sharing or improper use of keys, may result in disciplinary action. The registered key holder will be held accountable for any security breaches related to their assigned keys.

This policy ensures a robust approach to maintaining the security and integrity of our facilities while fostering a culture of accountability.

Please refer to the Business Continuity Plan for further actions in the event of theft or burglary.

Crystal Health Group's Staff
On commencement of employment, Crystal Health Group's staff are provided with building/office access security codes and an official ID card. On termination of employment, all keys and ID cards must be returned as part of the Staff Registration and Exit Policy.

All Crystal Health Group's staff are required to sign in and out of Crystal Health Group's office using the signing-in book. Official Crystal Health Group's staff ID cards must be worn at all times whilst on the premises.

Emergency Procedures
Fire emergency arrangements are detailed in Crystal Health Group's Fire Evacuation Policy. All other emergencies are covered in the Business Continuity Plan.

5.10 PCI Compliance

Crystal Health Group handles sensitive cardholder information daily. Sensitive Information must have adequate safeguards in place to protect them, to protect cardholder privacy, to ensure compliance with various regulations and to guard the future of the organisation.

Crystal Health Group commits to respecting the privacy of all its customers and to protecting any data about customers from outside parties. To this end, management are committed to maintaining a secure environment in which to process cardholder information so that we can meet these promises.

Employees handling Sensitive cardholder data must ensure:

- Handle Company and cardholder information in a manner that fits with their sensitivity;
- Protect sensitive cardholder information;
- Always leave desks clear of sensitive cardholder data and lock computer screens when unattended;
- Call recording must be paused when obtaining card data.
- Crystal Health Group have a process in place to monitor the PCI DSS compliance status.
- No third parties will have access to payment card account numbers.
- Quarterly internal vulnerability scans must be performed by internal staff and the scan process will include that rescans will be done until all High vulnerabilities are resolved.
- To start a vulnerability scan using Crystal Health Group's approved Bit Defender anti-virus software:
    1. Open the main application window.
    2. In the lower part of the main window, click the More Tools button.
    3. Go to the Manage applications section.
    4. Click the Vulnerability Scan link to open the Vulnerability Scan window.
    5. In the Vulnerability Scan window, click the Start scan button.
    6. Inform the ICT Manager of any vulnerabilities found with applications or the operating system.

The ICT Manager is responsible for attesting the company's PCI compliance status on an annual basis. Monthly spot checks of call recordings will take place and the findings will be reviewed at quarterly management review.

5.11 Cloud Services and Secure Development

Crystal Health Group uses a limited number of secure cloud services (e.g. Swiftcase, Daktela CRM), managed under approved supplier and change control processes. Secure development and configuration controls are applied where custom code or integration work is performed. These include access controls, versioning, approval workflows, and use of hardened production environments. The use of personal cloud accounts for any work-related data storage is strictly prohibited.

6. Version Control

Previous Version	Changes	Last Effective Date
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	10/09/2025
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
v06.08.24	Section 5.1 • Addition of reference to Statement of Applicability document. Section 5.3 • Update to Sample Collection Network Password Section 5.7 • Addition of Only approved Crystal Health Group assets • Addition of third party supplier in the disposal of ICT assets.	20/09/2024
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
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

6. Version Control

Previous Version	Changes	Last Effective Date
v03.03.20	• Addition of Section 5.10 ‘PCI Compliance’	02/06/2021
v02.04.18	• Update to Section 5.3 - Password Protection. Sub-section ‘Electronic Documents Passwords’	11/03/2020
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
NEW	• N/A	N/A

7. Authorisation

Name John McChrystal

Position Director

Signed

Date 11/09/2025