Data Protection & Privacy Policy

Effective from: 15-02-26
Review date: 15-04-27

Summary of this policy

This Data Protection & Privacy Policy sets out Chelton's commitment to safeguarding personal data in compliance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (as amended by the Data (Use and Access) Act 2025), Privacy and Electronic Communication Regulations (PECR), and ISO/IEC 27001 principles. It further integrates governance controls for the safe, ethical, and secure use of Artificial Intelligence (AI) within Chelton's products and services supplied to UK government.

Purpose of this policy and how to comply

The purpose of this Data Protection & Privacy Policy is to outline Chelton's commitment to processing personal data in a lawful, fair, and transparent manner.

This policy applies to all Chelton employees, workers, consultants, contractors, suppliers, vendors and third parties who process personal data on behalf of Chelton and are expected to handle personal data lawfully, fairly, securely, and only in approved systems.

You must only use what's necessary, retain it briefly, and dispose of it securely unless any other legal basis exists for continuing to process personal data. You must report any suspected or actual personal data incident immediately to the Data Privacy Office, ensure all vendors, suppliers and third parties follow this policy and only use them where a data processing agreement (DPA) is in place prior to the processing of personal data.

Mandatory compliance with this policy

Infringement of this Data Protection & Privacy Policy may result in disciplinary action, including termination of employment. All employees are under a duty comply with this policy and to report any concerns immediately to the Data Privacy Office.

Non-compliance with this policy by contractors, suppliers, vendors and third parties will be investigated by the Data Privacy Office and could result in termination, depending on the severity of non-compliance with this policy.

If you're unsure about compliance with any part of this policy, please seek guidance and support from the Data Privacy Office.

Actions and responsibility

The Data Privacy Office owns this policy, ensures legal accuracy, monitors compliance, advises on data protection and privacy duties, and leads breach response. Follow Data Privacy Office guidance on any data protection and privacy matter. The Chief Information Officer (CIO) supports compliance by implementing the necessary technical, organisational measures and physical security measures to ensure compliance with this policy

Version approval

Version	Compiled by	Reviewed by	Approved by
1.0	Angelo Faria	Fawad Siddiq	Interim DATA PRIVACY OFFICE
1.1	Ardi Kolah	CIO/Head of Cyber Security	SLT

Revision History

Version	Key Changes	Effective Date
1.0	Initial version to align Chelton's procedures to ISMS	02/01/2026
1.1	Revised in alignment with the Data Protection & Privacy Target Operating Model (TOM)	04/02/2026

Acronyms	
ADM	Automated Decision Making
AI	Artificial Intelligence
CIO	Chief Information Officer
DPA	Data Processing Agreement
DPA 2018	Data Protection Act 2018
DPIA	Data Protection Impact Assessment
DSAR	Data Subject Access Request
DUA Act 2025	Data (Use and Access) Act 2025
EEA	European Economic Area
GDPR	General Data Protection Regulation
ICO	Information Commissioner's Office (now known as the Information Commission)
ISMS	Information Security Management System
LIA	Legitimate Interests Assessment
PECR	Privacy and Electronic Communications Regulations
RoPA	Records of Processing Activities
UK GDPR	UK General Data Protection Regulation

Contents

1. Scope

This policy applies to the full lifecycle of personal data of employees, clients, contractors, suppliers, vendors and third parties processed by Chelton and includes the creation, collection, transmission, sharing, storage and secure disposal of personal data – whether in hard copy or in electronic formats.

2. Compliance with this Policy

Compliance with this Data Protection & Privacy Policy is MANDATORY. All processing of personal data must be carried out lawfully, fairly, and securely, using only approved systems and methods. The processing of personal data shall be limited to what is necessary for the specified purpose, retained only for the minimum period required, and disposed of securely in accordance with this Data Protection & Privacy Policy.

Where there is any uncertainty regarding the lawful basis for processing personal data or the interpretation and/or application of this policy, please refer directly to the Data Privacy Office for guidance and support. Any suspected or actual personal data incident must be reported immediately to the Data Privacy Office for investigation.

All vendors and third parties processing personal data on behalf of Chelton must comply with this Data Protection & Privacy Policy. Third-party processors can ONLY be engaged where there is a valid Data Processing Agreement (DPA) and appropriate contractual/ security safeguards are in place. For further advice and support, please contact the Data Privacy Office.

3. Explanation of terms used in this policy

Anonymised Data	The requirements of data protection and privacy do not apply to anonymised information, i.e. data that cannot identify an individual. Anonymised data refers to personal data has been rendered anonymous in such a manner the data subject is no longer identifiable.
Automated Decision-Making (ADM)	When a decision is made which is based solely on Automated Processing (including profiling) which produces legal effects or significantly affects an individual's rights. The UK GDPR/Data Protection Act 2018 (as revised by the Data (Use and Access Act) 2025 prohibits Automated Decision-Making (unless certain conditions are met) but not Automated Processing. In accordance with the Data (Use and Access) Act 2025, data subjects have the right to meaningful human intervention, the right to make representations, and the right to contest

	decisions based solely on automated processing or artificial intelligence that produce legal or similarly significant effects.
Automated Processing	Any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to an individual, to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Profiling is an example of Automated Processing.
Company	Chelton Ltd
Consent	Agreement which must be freely given, specific, informed and be an unambiguous indication of the data subject's wishes by which they, by a statement or by a clear positive action, signify agreement to the processing of personal data relating to them. Consent must be granular or unbundled from other terms and must be specific for each processing activity.
Data Controller	Chelton and employees ('business managers') engaged in managing the operations of the company and who determine when, why and how to process personal data. The Data Controller is responsible for compliance with relevant UK data protection and privacy laws, advised and guided by the Data Privacy Office.
Data Protection Impact Assessment (DPIA)	Tools and assessments used to identify and mitigate high/very high risks of a data processing. DPIA can be carried out as part of Privacy by Design and should be conducted for all major system or business change programmes involving the processing of personal data.
Data Privacy Office	Supports the senior leadership team on all privacy and data protection obligations, monitors compliance with UK and international laws and regulations and maintains policies, processes and procedures (including the use of AI) including Data Protection Impact Assessments (DPIAs), training and awareness and is the key contact point for all employees and the Information Commission.
Data Subject	A living identified or identifiable individual about whom the company holds personal data. Data Subjects may be nationals

	or residents of any country and may have legal rights regarding their personal data both within and outside the UK.
Data Subject Access Request (DSAR)	A request made by an individual to obtain confirmation as to whether Chelton processes their personal data and, where that is the case, to receive a copy of such personal data and related information. Chelton will carry out reasonable and proportionate searches to locate the personal data falling within the scope of the request. The statutory response period commences only once Chelton has verified the requester's identity and, where necessary, clarified the scope of the request. The right of access is a qualified right, and there may be circumstances in which personal data cannot be disclosed, in whole or in part, due to applicable legal exemptions or restrictions.
Data Processor	A person or organisation that carries out data processing activities on the written and explicit instructions of the Data Controller. This will include contractors, vendors and third parties. The Data Processor is jointly and severally liable for any personal data breaches that occur alongside the Data Controller.
DPA 2018	The Data Protection Act 2018 (c. 12) supplements and gives effect to the UK GDPR in UK law and provides additional provisions, exemptions, and enforcement powers relating to the processing of personal data.
Data (Use and Access) Act 2025	The Data (Use and Access) Act 2025 (c. 18) amends the UK General Data Protection Regulation, the Data Protection Act 2018, and related legislation to reform aspects of the UK data protection and privacy framework.
UK GDPR	Regulation (EU) 2016/679 of the European Parliament and of the Council, as it forms part of UK domestic law by virtue of section 3 of the European Union (Withdrawal) Act 2018 (as amended). Common short title: UK General Data Protection Regulation (UK GDPR)
Information Commission	The UK's independent regulator for data protection and electronic communications, established by the Data (Use and Access) Act 2025, with responsibility for enforcing the UK GDPR, the Data Protection Act 2018, and the Privacy and

	Electronic Communications (EC Directive) Regulations 2003. Formerly known as the Information Commissioner's Office (ICO).
Personal Data	Any information identifying a data subject or information relating to a data subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. Personal Data includes Special Categories of personal data and pseudonymised personal data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour. You don't always need to have the name of someone for the data to qualify as personal.
Personal Data Breach	Any act or omission that compromises the security, confidentiality, integrity or availability of personal data or the physical, technical, administrative or organisational safeguards that we or our third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure, alteration or acquisition, of personal data is a Personal Data Breach, reportable to the Information Commission.
PECR	The Privacy and Electronic Communications (EC Directive) Regulations 2003 (SI 2003/2426), which regulate electronic marketing, cookies and similar technologies, and the security and confidentiality of electronic communications in the UK, and which operate alongside the UK GDPR and the Data Protection Act 2018.
Privacy or Data Protection Incident	Any actual or suspected event involving the misuse, loss, unauthorised access to, disclosure of, or failure to adequately protect personal data, or any other non-compliance with Chelton's Data Protection & Privacy Policy. Following investigation by the Data Privacy Office, a Privacy or Data Protection Incident may be classified as a Personal Data Breach and, where required by law, may be reportable to the Information Commission. For the purposes of this policy, a privacy or data Protection incident is treated as a security breach.

Privacy by Design	The principle that appropriate technical and organisational measures are implemented, at the time of determining the means of processing and throughout the personal data processing lifecycle, to integrate data protection safeguards and to protect the rights and freedoms of individuals.
Privacy Notice	A separate and clearly identifiable legal document for different categories of individuals, including employees, contractors, suppliers, vendors and other third parties, where their personal data is processed in different contexts. The Data Privacy Notice, provided to individuals under UK data protection and privacy laws, explains the legal basis for processing their personal data, how and why their personal data is collected, used, stored, shared, and protected, and sets out their rights and how to raise concerns with the company and make a complaint to the independent Regulator, the Information Commission.
Privacy Policy	A document that explains how an organisation protects personal data and meets its legal data protection obligations.
Processing	Any activity that involves the use of personal data, it includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring personal data to third parties. Viewing personal data on a screen also falls within the definition of processing.
Profiling	Any form of automated processing of personal data consisting of the use of such data to analyse, assess, or make predictions about an individual, to evaluate or classify personal aspects relating to that individual, such as behaviour, performance, preferences, characteristics, location, or interests.
Pseudonymised data	Personal data which has been processed so that it cannot be attributed to a specific data subject without the use of additional information (e.g. a key), where that additional information is kept separately and protected by appropriate safeguards. Pseudonymised data is not anonymised and continues to be treated as personal data for the purposes of UK data protection and privacy laws.

Records of Processing Activities (RoPA)	The formal records required under UK data protection and privacy laws that document the company's personal data processing, including who processes the personal data, for what purposes, what personal data and data subjects are involved, where the personal data is stored or transferred, how long it is retained, and the security measures applied to protect it.
Security Breach	Any actual or suspected event that compromises, or is reasonably likely to compromise, the confidentiality, integrity, or availability of Chelton's information, systems, or services, including all privacy or data protection incidents and any personal data breach, whether caused by accidental or unlawful acts or omissions.
Sensitive Personal Data or Special Categories of Personal Data	Information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data.
Systems	Computer networks, hardware, software/applications and tools used to facilitate communications, store or transmit information and support the business of the company.

4. Chelton's Data Protection & Privacy Principles

The following Data Protection & Privacy Principles are fundamental to the company meeting its legal and regulatory obligations:

4.1 FIRST PRINCIPLE: Lawfulness, Fairness and Transparency

We will only process personal data lawfully, fairly and in a transparent manner.

What you must do:

- Only process personal data where we have lawful grounds and legitimate business reasons to do so (Lawfulness and Fairness).
- Be transparent and inform individuals as to what data about them we collect and how we will use, share and destroy it (Transparency).

4.2 SECOND PRINCIPLE: Purpose Limitation

We'll collect personal data only for specified, explicit and legitimate purposes and we'll not process it further in any manner incompatible with those purposes.

What you must do:

- You must specify the purposes (i.e. reasons) why you're collecting and using personal data before the collection. You can't and and mustn't use personal data you've collected for a particular purpose (as usually described in the privacy notice, policy or statement) for anything else, unless all relevant legal and regulatory requirements regarding the additional use(s) are complied with.

- The individuals concerned have been informed and, where required, their consent has been obtained before their personal data can be used for any new, different or incompatible purposes from those disclosed in our privacy notices when we first obtained their personal data.

4.3 THIRD PRINCIPLE: Data Minimisation

We'll only process personal data that's adequate, relevant and limited to what's necessary in relation to the purposes for which it is processed.

What this means you must do:

- Collect and retain only the data that you really need to carry out a specific purpose or function (that is even if the information would be useful to know/have).
- Not record personal data for the sake of it.
- Delete/destroy (or anonymise as relevant and appropriate) any personal data no longer needed in accordance with Chelton's Records Retention and Deletion Policy & Schedule or other related policies and procedures.

4.4 FOURTH PRINCIPLE: Accuracy

We'll ensure that the personal data we process is accurate and, where necessary, kept up to date.

What you must do:

- Check and assess the accuracy of any personal data that you process at the point of collection (or request validation about its accuracy if the data is received from another party), and thereafter.

- Update, correct or delete (as relevant) without delay and in accordance with relevant processes and procedures any personal data found to be inaccurate or out-of-date.

4.5 FIFTH PRINCIPLE: Storage Limitation

We'll only keep personal data for as long as necessary for the purpose(s) for which it's required to be processed.

What you must do:

- Classify and retain personal data in accordance with the company's Records Retention and Deletion Policy and ensure you can justify why you need to retain the relevant personal data.
- Ensure that personal data is securely disposed of in accordance with the company's Records Retention and Deletion Policy or is anonymised, as relevant, at the end of the appropriate period, unless otherwise required or permitted (e.g., a disposal hold, legal exemption).
- Ensure that any contractors/vendors/third parties that process personal data on our behalf must also delete or return such personal data as applicable.

4.6 SIXTH PRINCIPLE: Data Security - Integrity and Confidentiality

We'll ensure that we process personal data in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage.

What you must do:

- Protect the confidentiality, integrity and availability of personal data, through all stages of the data lifecycle (from the point of creation to the point of disposal).
- Confidentiality means that only people who have a need to know and are authorised to use the personal data can access it.
- Integrity means that personal data is not altered, corrupted, damaged or lost because of unlawful or unauthorised processing; and
- Availability means that only authorised users can access the personal data when they need it and only for authorised purposes.
- Ensure that we have appropriate physical and technological security measures to protect the personal data whether it is on or off-site. The level of security required will depend on the nature of the personal data (e.g., particular care must be exercised in protecting sensitive personal data) and the potential harm that could be caused by the unlawful, unauthorised

or accidental processing of personal data. For further guidance please refer to the relevant IT, security and other related policies.

- Train all Chelton employees on their data protection and privacy obligations on a periodic basis. The training provided must take into consideration the risk presented by appropriate factors such as the nature and volume of personal data, the roles and activities of employees.
- Follow all policies, processes, procedures and guidelines we put in place to maintain the security of all personal data.
- Ensure that any contractors/vendors/third parties have appropriate security measures in place and a contract with Chelton which details the data processing activities they will be carrying out, as well as their data protection obligations in relation to the personal data they will be accessing and processing (if such processing is applicable).
- Ensure that a secure method of transit is employed when personal data is transferred from one location to another.

4.7 SEVENTH PRINCIPLE: Data Protection by Design and by Default

We ensure that we'll integrate data protection concerns into every aspect of our processing activities.

What you must do:

- Systems, processes, business practices, products and services must be designed to protect individuals' privacy.
- You must consider and respect all Chelton's Data Protection & Privacy Principles.
- You must embed data protection and privacy-protective mechanisms into the fundamental design of systems, processes, operations, products and services and adopt appropriate measures.
- You must always carry out a Data Protection Impact Assessment (DPIA) for processing that is likely to result in a high-risk to the rights and freedoms of individuals. Since DPIAs help identify and minimise the data protection risks of a project, you should carry out appropriate assessments on all major projects that involve the processing of personal data. For guidance and support, contact the Data Privacy Office.

4.8 EIGHTH PRINCIPLE: Transfer Limitation

We'll ensure that suitable safeguards are in place before transferring personal data to another country (where relevant).

What you must do:

- You must ensure that any personal data which the company is responsible for will be adequately protected in the country of destination when transferred across border and that requirements regarding transfers or data location (localisation) are complied with. For guidance and support, contact the Data Privacy Office.

4.9 NINETH PRINCIPLE: Respect for Individuals' Rights

We'll observe the rights afforded to individuals under their local privacy and data protection laws which may include:

- The right to receive certain information about how we process their personal data (*Right to Know*);
- The right to request access to their personal data that we hold (*Right of Access*);
- The right has inaccurate or missing information corrected or updated (*Right to Rectification or Correction*);
- The right to have personal data deleted when certain circumstances apply (e.g., if it is no longer needed in relation to the purposes for which it was collected or processed) (Right to Erasure (Right to be Forgotten));
- The right to restrict or object to processing in specific circumstances (Right to Restriction of processing);
- The right to object to any decisions we may make based solely on Automated Processing, including profiling (Right to Object to automated individual decision-making, including profiling);
- The right to withdraw consent to processing at any time where processing is based on consent (including to withdraw any marketing relating consents) (Right to withdraw consent);
- The right to challenge processing which has been justified based on our legitimate interests or in the public interest (Right to Object);
- The right to be notified of a personal data breach which is likely to result in high risk to their rights and freedoms (Right to Notification);
- The right to make a complaint to the Information Commissioner's Office (Right to Complain);
- The right, in limited circumstances, to receive or ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (Right to Portability or transfer); and
- The right that we will not discriminate against you in any way if you choose to exercise any of the rights that apply to you (Right to Non-discrimination).

What you must do:

- Ensure that all queries relating to data protection and privacy issues are promptly and transparently dealt with in accordance with regulatory requirements.
- Appropriate procedures must be in place to allow employees, contractors/vendors/third parties to address any of the above in a compliant manner.

4.10 TENTH PRINCIPLE: Accountability

We take responsibility for complying with the Data Protection & Privacy Principles at the highest management level and throughout our company and can demonstrate compliance.

What you must do:

- Take responsibility for what we do with personal data and can demonstrate how you comply with the Data Protection & Privacy Principles and the steps you've taken to protect personal data and respect the rights of the individuals concerned.
- Understand and comply with the relevant policies, processes and procedures.
- Are aware of your duties and responsibilities and understand the role you play in meeting our Data Protection & Privacy obligations.
- Must implement appropriate technical, organisational and contractual measures and maintain records in an effective manner, to ensure compliance with data protection and privacy principles. The company is responsible for, and must be able to demonstrate, compliance with the data protection and privacy principles.
- Keep full and accurate records of all our data processing activities, also known as 'Records of Processing Activities'. For guidance and support, contact the Data Privacy Office.
- Keep accurate records of data subjects' consents and ensure procedures are in place for obtaining consents in accordance with the company's record-keeping guidelines.
- Embed a privacy/data protection by design and by default approach in the way you develop a project, a system or an operation which will involve the processing of personal data. This means that appropriate data protection and privacy measures are implemented throughout the personal data lifecycle.
- Report to the Data Privacy Office, without undue delay, any concerns you have or details of any potential personal data incidents that will require to be investigated by the Data Privacy Office.

5. Legal Basis for Processing Personal Data

Chelton processes personal data only where a valid legal basis applies in accordance with UK data protection law. For each specific processing purpose, Chelton identifies and relies upon the most appropriate legal basis. Depending on the nature and purpose of the processing, this may include one of the following legal grounds:

- **Consent:** The data subject has given freely given, specific, informed, and unambiguous consent to the processing of their personal data for one or more specified purposes.
- **Contract**: Processing is necessary for the performance of a contract to which the data subject is a party, or to take steps at the request of the data subject prior to entering a contract.
- **Legal Obligation**: Processing is necessary for compliance with a legal obligation to which Chelton is subject.
- **Vital Interests**: Processing is necessary to protect the vital interests of the data subject or of another natural person, for example in emergency or life threatening situations.-threatening situations.
- **Public Interest or Official Authority**: Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in Chelton.
- **Legitimate Interests**: Processing is necessary for the purposes of Chelton's legitimate interests or those of a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject. Where this legal basis is relied upon, Chelton will carry out and document an appropriate Legitimate Interests Assessment (LIA).

6. AI Governance and Ethics Framework (2026)

Chelton recognises that Artificial Intelligence (AI) and automated systems will play an increasing role in the processing of personal data, including activities involving analysis, profiling, decision support, and risk assessment. While AI can deliver operational benefits, it also presents heightened risks to individuals' rights and freedoms, including risks relating to transparency, fairness, discrimination, accountability, and security.

Accordingly, Chelton applies this AI Governance and Ethics Framework to ensure that the use of AI systems (where appropriate) involving personal data is lawful, fair, transparent, and aligned with the UK GDPR/Data Protection Act 2018, and this Policy. This framework is designed to embed data protection principles into the design, deployment, and ongoing use of AI systems.

6.1 Human-in-the-Loop (HITL)

All AI systems that produce, support, or inform decisions with legal, security, or similarly significant effects on individuals must incorporate meaningful human oversight. From a data protection and privacy perspective, this ensures that:

- decisions are not based solely on automated processing where this would be unlawful or inappropriate.
- individuals' rights to challenge decisions, obtain human intervention, and receive explanations are respected; and
- accountability for processing remains clearly assigned to human decision-makers, rather than delegated entirely to automated systems.
- Human oversight must be sufficient to enable review, correction, and override of AI generated outputs where necessary.-generated outputs where necessary.

6.2 Algorithmic Transparency

Chelton maintains an inventory of all AI tools and systems used in the processing of personal data, including their purpose, data inputs, and deployment context. In support of transparency obligations:

- Chelton must be able to explain, at an appropriate level, the logic, significance, and envisaged consequences of AI assisted processing to affected individuals.-assisted processing to affected;
- transparency information must be capable of supporting Data Privacy Notices, DSAR responses, and complaints handling; and
- opaque or "black-box" systems will not be used where they prevent Chelton from meeting its transparency and accountability obligations.
- Algorithmic transparency supports individuals' rights and underpins trust in Chelton's data processing activities.

6.3 Bias Mitigation and Fairness

Chelton takes proactive steps to identify and mitigate bias and discriminatory outcomes arising from AI systems that process personal data. In particular:

- fairness audits are conducted on training data, models, and outputs, especially where processing involves profiling or high-risk contexts;
- personal data used to train or test AI systems must be relevant, accurate, and representative, in line with data minimisation and accuracy principles; and
- outcomes are monitored to ensure that AI assisted processing does not result in unlawful discrimination or unjustified adverse impacts on

individuals or groups.-assisted processing does not result in unlawful discrimination or unjustified adverse impacts on individuals or groups.
- Bias mitigation is a core component of Chelton's obligation to process personal data fairly and lawfully.

6.4 Security by Design

AI systems used by Chelton are subject to security by design and security by default principles, consistent with Chelton's information security framework. From a data protection perspective:

- AI models and supporting infrastructure must be protected against unauthorised access, data leakage, model inversion, and adversarial manipulation;
- resilience and reliability testing is conducted to reduce the risk of data breaches or integrity failures; and
- security controls are proportionate to the nature, scope, context, and risks of the processing.
- Security safeguards are essential to protecting the confidentiality, integrity, and availability (CIA) of personal data processed by AI systems.

6.5 Data Protection Impact Assessments (DPIAs)

A Data Protection Impact Assessment (DPIA) is mandatory for all new AI systems or material changes to existing systems where personal data is processed. DPIAs ensure that:

- risks to individuals' rights and freedoms are identified, assessed, and mitigated before deployment;
- AI specific risks (including profiling, automated decision making, bias, and transparency risks) are explicitly addressed; and-specific risks (including profiling, automated decision-making, bias, and transparency risks) are explicitly addressed; and
- the Data Privacy Office is involved at an early stage, in line with privacy by design and by default obligations.
- No AI system involving personal data may be deployed where residual risks remain high and unmitigated.

7. Roles and Responsibilities

Clear definition of roles and responsibilities is essential for effective data protection and privacy governance. By assigning specific responsibilities to key roles such as the Data Privacy Office, Data Controller, Data Processor, management, and employees, Chelton ensures:

- compliance with legal and regulatory requirements;
- consistent application of security controls and privacy principles; and
- rapid and coordinated response to data protection incidents.

Roles	Responsibilities
Data Privacy Office	The Data Privacy Office oversees Chelton's data protection and privacy Target Operating Model and ensures compliance with applicable data protection and privacy laws. The Data Privacy Office is the key point of contact for data subjects and regulatory authorities.
Data Controller	Determines the purposes and means of processing personal data. The primary decision-maker on what personal data is collected and why. The controller (business owner) holds the ultimate responsibility for ensuring all processing activities comply with Chelton's Data Protection & Privacy Principles.
Data Processors	Processes personal data on behalf of a Data Controller. They act solely on the documented explicit instructions of the Data Controller and don't determine the purpose or means of data processing. Their key responsibilities include implementing appropriate security measures, assisting the Data Controller with data subject rights requests, notifying the Data Controller of data protection and privacy issues and responding to the Data Privacy Office for assistance to investigate such issues.
Employees	All employees are responsible for following Chelton's data protection and privacy policy and procedures and for safeguarding personal data in their day-to-day activities. Employees must report any data breaches or suspected breaches to the Data Privacy Office immediately.
Management	Senior management is responsible for ensuring that data protection is integrated into Chelton's overall governance framework and that adequate resources are allocated to implement this policy.

These responsibilities form the foundation for helping to create a culture of data confidence within Chelton and maintain continuous improvement in data protection and privacy practices.

Accountability metrics:

- Managers must ensure quarterly compliance checks within their teams.
- Data Privacy Office to maintain an incident and reportable data breach log with regular independent reporting to the Board in according with the Target Operating Model (TOM).

8. Monitoring and Review

This policy will be reviewed annually during ISMS management review meetings and updated based on audit findings, regulatory changes, and business needs, in accordance with Chelton's internal audit procedures (CMP 221-14).

9. Other related documents

- Data Privacy Office Playbook (February 2026)
- IT SecPOL 2023 ISP
- IS 301 - Access Control Policy
- IS 203 - Data Classification Policy
- CMP 221-14 Quality Audits Assessments (CMP 221-14)
- CMP 101-2 Risk Management (CMP 101-2)
- Vendor Risk Management & Toolkit (March 2026)
- Records Retention and Deletion Policy & Schedule (March 2026)
- Data Privacy Policy (March 2026)
- Data Privacy Notice – Employees (April 2026)
- Data Privacy Notice - Customers (April 2026)