Group Policy

Information Security

02 October 2025

Reference:	**Group Policy – Information Security**
Issue Date:	02/10/2025
Classification :	Internal

COGNITA

THRIVE IN A RAPIDLY EVOLVING WORLD

Key Facts

- Cognita must comply with all applicable laws, regulations, and contractual obligations related to information security.
- Group Cyber Security defines baseline security controls and monitors compliance across all regions, schools, and technologies.
- The Group aligns with the NIST Cyber Security Framework and undergoes internal and third-party cyber security maturity assessments (at least every three years).
- All employees must complete cyber security training (at least yearly) and follow the Digital Acceptable Use Policy.
- Regions must integrate and manage training through their HR platforms and follow up on non-compliance.
- Regions and schools must maintain accurate inventories of digital assets and assess cyber risks in accordance with Cognita Cyber Risk Management Frameworks.
- All critical and high-risk suppliers must be assessed for cyber security risk in accordance with Group defined requirements.
- Identity and access management must follow Group requirements, including Multi-Factor Authentication (MFA), least privilege, and Role Based Access Control (RBAC).
- Sensitive and critical data must be classified, protected, and managed securely throughout its lifecycle.
- Systems, platforms, infrastructure, and email must meet security requirements defined in the Group Cyber Security Control Set and be regularly maintained.
- Security logging, event detection, and incident response must be implemented to ensure rapid detection and response to threats.
- Regular system backups must be performed, securely stored, and tested to support recovery and business continuity.
- Bring Your Own Device (BYOD) use is permitted for staff only if devices are enrolled in a Group approved Mobile Device Management (MDM) solution.
- Roles and responsibilities are clearly defined for Cyber Security, IT, Legal, and employees across all levels.

Document Control

Title	Group Policy – Information Security
Author	James Tallon (JT)
Owner	Reena Shah (RS)
Subject	Cyber Security Information Security
Classification	Internal
Next Review Due Date	02 October 2026

Revision History

Revision Date	Reviser	Previous Version	Description of Changes
-	JT	-	Creation of policy

Document Approvals

Name	Title	Date
Cyber Security Steering Group (CSSG)	Senior Governing Body for Cyber Security Across Cognita (Retired Sep 2025)	24/06/2025
Group Executive Team	Group Executive Leadership Team	02/10/2025

Document Distribution

Role(s)	Method
Group IT	Email
Regional IT and leadership	Email
Group Executive Team	Email
Group and Regional Legal Team	Email
Group and Regional Communication Team	Email
Group and Regional Safeguarding Team	Email
Cognita Staff	Cognita People, Cyber Training Module

Associated Documents

Title
Group Policy - Cyber Security Incident Response
Group Cyber Security Control Set
Group Policy – Acceptable Use of Digital Assets

Contents

1. Definitions

Availability refers to ensuring that IT systems, software, and digital resources are accessible and operational when needed by authorised users. This includes maintaining and safeguarding systems to prevent downtime, interruptions, or disruptions that could impede access to essential digital assets.

Cognita Group (the "Group") refers to Cognita Holdings Limited and its subsidiaries, affiliated schools, and related entities globally. This includes all educational institutions, administrative offices, and operational units under the Group's ownership or control.

Confidentiality refers to the obligation to protect sensitive information from unauthorised access, disclosure, or dissemination. This includes ensuring that all data, communications, and records related to the Group, its operations, and its stakeholders are kept secure and only accessible to individuals who are authorised to view or handle such information.

Data Residency refers to the requirement for certain data to be stored, processed, or accessed within a specific geographic location. This is typically driven by legal, regulatory, or contractual obligations applicable in the country where the data is collected or used.

Digital Assets refers to all IT systems, software, data, and related resources that belong to or are part of the Groups digital ecosystem. This includes, but is not limited to, hardware, applications, databases, networks, and any other electronic or digital resources utilised by the school.

Employees refer to all individuals within Cognita Group, including full-time and part-time staff, contractors, consultants, and any other personnel engaged for short-term or specific projects. This encompasses anyone who performs duties or provides services on behalf of the Group, regardless of their employment status or duration of engagement.

Group IT is a head office function that sets group wide IT requirements and has overall visibility across Cyber Security, Infrastructure, Applications, and IT Service Management (ITSM). It ensures alignment with organisational goals, providing guidance and support to regional teams and business units.

Integrity refers to the accuracy, consistency, and reliability of information and systems. It involves safeguarding data from unauthorised alteration or corruption and ensuring that all digital assets and communications remain unaltered and trustworthy throughout their lifecycle

Personal Data / Personally Identifiable Information (PII) refers to any information that relates to an identified or identifiable individual. This includes, but is not limited to, names, identification numbers, contact details, location data, and online identifiers. Specific definitions and legal requirements may vary by country.

Technology / System Owner refers to the individual or team responsible for the management, security, and compliance of technology assets, including applications, SaaS

systems, and infrastructure. They are accountable for ensuring these technologies align with business objectives, meet security standards, and address any associated risks.

2. Policy Review Cycle

2.1 This policy will be reviewed annually, or sooner if triggered by significant security incidents, regulatory changes, or major technology updates, as determined by the Group Cyber Security Team or Management. The purpose of this review is to evaluate the effectiveness of the policy in addressing evolving security threats, technological advancements, and changes in regulatory requirements.

3. Purpose

3.1 The purpose of this policy is to establish Cognita's approach to managing and safeguarding its information assets. It sets clear expectations and responsibilities regarding the protection of information assets, with the following objectives:

- To protect Cognita's digital assets and ensure their confidentiality, integrity, and availability.
- To manage information security risks and minimise potential impacts on operations and reputation.
- To ensure compliance with relevant regulations, industry standards, and contractual obligations.
- To support the Group's commitment to proactive risk management and robust security practices.

4. Scope

4.1 This Policy applies to all Cognita Group companies and schools worldwide ("Cognita" or "Group") and to all Employees, whether permanent or temporary, including teachers, staff and administrators.

4.2 All exceptions to this policy must be requested using the Cyber Security Exception request form. Exceptions will be evaluated on a case-by-case basis and approved by the Group Cyber Security Team. Escalation to the Cognita Group Executives will be required if a significant risk due to non-compliance is identified.

5. Policy Statements

5.1 Compliance with Legal and Regulatory Requirements

5.1.1 The Group Cyber Security Team must maintain oversight of legal and regulatory compliance requirements relating to information security across the Group.

5.1.2 Regions with support from schools and technology owners are responsible for identifying and understanding their local legal, regulatory, and contractual obligations relating to information security, and ensuring these are met.

5.1.3 Where a conflict arises between a Group defined requirement and a legal or regulatory obligation, the legal or regulatory obligation must take precedence. Regions and schools must identify such conflicts and notify the Group Cyber Security Team in a timely manner. The Group Cyber Security Team, in consultation with Group / Regional Legal and other relevant stakeholders, is responsible for determining the resolution and escalation path.

5.1.4 Cognita Group aligns its information security practices with industry recognised frameworks, including the NIST Cyber Security Framework (CSF), to guide the development of security controls.

5.1.5 The Group Cyber Security Team will conduct internal assessments of the Group's cyber security maturity. In addition, an independent third-party assessment must be conducted at least every three years to evaluate the overall maturity and alignment with best practices.

5.1.6 Regions and schools must ensure that any regulatory or data breach notifications are made to regulators and affected parties within the legally mandated timelines for their jurisdiction. Responsibility for meeting these obligations rests with the regional or local teams, supported by Group Legal as required.

5.2 Group Defined Controls, Processes, and Procedures

5.2.1 The Group Cyber Security Team must establish and monitor organisation wide controls, processes, and procedures to ensure consistent and effective management of information security across all regions, schools and technology.

5.2.2 Cyber security controls must align with regulatory requirements and industry practices. Control design and implementation should also consider the organisation's maturity level and be regularly reviewed to address evolving security risks.

5.2.3 All regions, schools and technology owners are required to adhere to these requirements, ensuring cohesive and unified security practices across the Group.

5.2.4 All regions, schools, and technology owners must provide accurate evidence of compliance with security controls within the timeframe specified by Group Cyber Security at the time of request, unless otherwise agreed.

5.3 Awareness & Training

5.3.1 The Group Cyber Security Team must develop and maintain security awareness and training programmes tailored to Cognita Group, ensuring they are made available to regions and schools for implementation through HR training platforms or other appropriate means.

5.3.2 The Group Cyber Security Team must monitor compliance statistics and track overall training completion, providing reports and escalations to Group and Regional IT Directors as required.
5.3.3 The Group Cyber Security Team must develop and maintain a Digital Acceptable Use Policy that covers all employees.
5.3.4 Regions are responsible for integrating Group Cyber Security training into their respective HR systems, ensuring all employees maintain compliance with the required training.
5.3.5 Regions are responsible for following up on non-compliance and taking the necessary actions to ensure all employees complete required training.
5.3.6 Regions must support the translation and feedback processes to ensure effective delivery of cyber security training and awareness across the Group.

5.4 Asset Management

5.4.1 The Group Cyber Security Team must develop and maintain baseline requirements for documenting and maintaining up to date digital asset inventories.
5.4.2 Regions, schools and technology owners must maintain accurate and up to date digital asset inventories in compliance with Group Cyber Security requirements.

5.5 Risk Management

5.5.1 The Group Cyber Security Team must define a Cyber Security Risk Management Framework in alignment with the broader Group Risk Management requirements. This includes establishing processes for regular cyber risk assessments, ensuring timely identification, evaluation, and mitigation of risks.
5.5.2 The Group Cyber Security Team must have visibility of all cyber security risk registers, ensuring they are integrated into the enterprise risk register as required.
5.5.3 Regions, schools, and technology owners must ensure that regular cyber risk assessments are conducted for high risk and critical systems, maintain accurate and up-to-date risk registers, and align their practices with the Group's framework and requirements.

5.6 Cyber Security Supply Chain Risk Management

5.6.1 The Group Cyber Security Team must define requirements for assessing third-party suppliers based on their assessed risk to Cognita Group.
5.6.2 The Group Cyber Security Team must have visibility and oversight of supplier risk management activities across Cognita Group.
5.6.3 Regions, schools and technology owners must assess suppliers in accordance with Group Cyber Security guidance and requirements, ensuring that suppliers are appropriately evaluated and managed based on the risk they represent to Cognita Group.

5.7 Vulnerability Management

5.7.1 The Group Cyber Security Team must maintain a vulnerability management tool to scan defined internal and external digital assets. The scope of assets to be scanned must be documented as part of the vulnerability management process and Group Cyber Security control set.

5.7.2 The Group Cyber Security Team must maintain a vulnerability management process to identify, validate, record and communicate vulnerabilities for both internal and external digital assets to responsible technology owners.

5.7.3 Each Region must ensure all internal and external digital assets are documented and shared with the Group Cyber Security Team for onboarding into the Group vulnerability management tool.

5.7.4 Regions, schools and technology owners are responsible for remediating vulnerabilities in line with Group Cyber Security requirements.

5.8 Identity, Management, Authentication and Access Control

5.8.1 The Group Cyber Security Team must define requirements for Identity and Access Management (IDAM) controls, which may include requirements for multi-factor authentication, least privilege access, and regular reviews of access rights to mitigate the risks of unauthorised access to sensitive information.

5.8.2 Regions, schools and technology owners must implement IDAM controls, ensuring that only authorised individuals have access to sensitive information, and that access is reviewed and updated regularly in accordance with Group Cyber Security requirements.

5.8.3 Regions, schools and technology owners must implement role-based access controls (RBAC) to ensure that access rights are assigned based on the role and responsibilities of the individual. Access must be granted according to the principle of least privilege, ensuring that individuals only have the minimum level of access necessary to perform their job functions.

5.8.4 Regions, schools and technology owners must develop appropriate human resource processes, ensuring hiring, onboarding and offboarding comply with business and security requirements.

5.8.5 Regions, schools and technology owners must ensure that physical access controls are considered and implemented based on the risk of unauthorised access.

5.9 Data Security

5.9.1 The Group Cyber Security Team must define a data taxonomy and classification matrix to ensure data can be appropriately classified.

5.9.2 Regions, schools and technology owners must classify and protect data in accordance with defined Group Cyber Security requirements, implementing appropriate security measures to maintain the confidentiality, integrity, and availability of all data.

5.9.3 Regions, schools and technology owners must ensure that secure data lifecycle practices are created and followed, including the classification, storage, handling, transfer, retention and destruction of data, commensurate with legal, regulatory and business requirements.

5.10 Device Security

5.10.1 The Group Cyber Security Team must define baseline security requirements to protect platforms and systems from known vulnerabilities and threats. These requirements are detailed in the Group Cyber Security Control Set and form the minimum-security requirements for devices.

5.10.2 Regions, schools and technology owners must implement defined security requirements for platforms under their responsibility, ensuring that security patches are applied, settings are configured securely, and authentication and authorisation controls are enforced in line with Group Cyber Security requirements.

5.10.3 Staff may use Bring Your Own Device (BYOD) for Cognita related work, provided the device is enrolled in a Group approved Mobile Device Management (MDM) solution that meets Group Cyber Security requirements. This requirement does not apply to student devices with the use of BYOD for students to be at the discretion of each school and region.

5.11 Platform, Technology & Infrastructure Security

5.11.1 The Group Cyber Security Team is responsible for defining baseline security requirements for all technology, including infrastructure, applications, SaaS systems, and other platforms, regardless of where they are hosted or managed.

5.11.2 The Group Infrastructure Team is responsible for defining and maintaining security requirements for core infrastructure components, ensuring that relevant controls are effectively designed, implemented, and monitored.

5.11.3 Technology owners, including regions and schools, must implement the defined security requirements across all systems and applications under their control. They must regularly monitor compliance and report status to the Group Cyber Security Team when requested.

5.11.4 Technology owners must assess and implement appropriate business continuity and disaster recovery measures based on the criticality of the systems and services they manage.

5.11.5 Technology owners must ensure networks and technology environments are securely configured, with appropriate segmentation and monitoring in place relative to the sensitivity and purpose of the systems involved.

5.12 Email Protection

5.12.1 The Group Cyber Security Team must define baseline security requirements for email systems to protect against threats such as phishing, malware, and

unauthorised access, ensuring secure and reliable email communication across the Group.

5.12.2 Technology and system owners must ensure that email protection is implemented to maintain the confidentiality, integrity, and availability of email communications and to prevent malicious content and email-based attacks.

5.13 Systems Backups

5.13.1 Technology and system owners must define backup requirements, based on system criticality and Group Cyber Security Requirements.

5.13.2 Regions, schools and technology owners must ensure system backups are implemented and maintained to ensure the availability and integrity of critical data and systems. Backups must be conducted regularly, securely stored, and tested for recovery to support business continuity and rapid restoration in the event of data loss, system failure, or disaster.

5.14 Security Logging

5.14.1 The Group Cyber Security Team must define security logging requirements.

5.14.2 Regions, schools and technology owners must ensure security logs are collected and maintained to ensure comprehensive monitoring of systems and network activities, supporting the detection, investigation, and response to security incidents and operational anomalies.

5.15 Event Detection

5.15.1 The Group Cyber Security Team is responsible for maintaining and managing the Group's event detection tools and capabilities, ensuring they are configured to detect security threats across the Group's environments.

5.15.2 Regions, schools and technology owners are responsible for maintaining continuous monitoring capabilities within their respective environments to ensure prompt detection and response to security threats.

5.16 Cyber Incident Response

5.16.1 The Group Cyber Security Team must define and maintain a Cyber Security Incident Response Policy.

6. Roles & Responsibilities

6.1 Group Executives

6.1.1 Review and approve the Group Information Security Policy to ensure it aligns with business objectives.

6.1.2 Support policy embedment across regions, ensuring appropriate funding and resources are available for implementation.

6.1.3 Accountable for ensuring teams receive adequate budget and support to comply with policy and control requirements set by the Group.

6.2 Group Cyber Security Team

6.2.1 Develop, maintain, and update the Group Information Security Policy in line with best practices and regulatory requirements.
6.2.2 Monitor and report on compliance with the policy across the Group.
6.2.3 Provide guidance, tools, and support to regional teams for consistent implementation of security controls.
6.2.4 Oversee security audits, assessments, and ongoing improvements to address emerging risks.

6.3 Group, Region and School IT Teams

6.3.1 Schools are directly accountable for implementing and evidencing compliance with the policy requirements applicable to their environment, in addition to supporting their regional teams.
6.3.2 Maintain an accurate inventory of IT and digital assets, ensuring appropriate security controls are applied based on classification and criticality.
6.3.3 Identify, document, and manage local information security risks, maintaining regional risk registers and reporting status to the Group Cyber Security Team.
6.3.4 Implement and operate technical, administrative, and physical security controls in alignment with the Group Information Security Policy and defined control requirements.
6.3.5 Provide and maintain secure IT infrastructure and systems to support compliance and business operations.
6.3.6 Collaborate with the Group Cyber Security Team to address identified vulnerabilities and emerging threats.
6.3.7 Implement local controls and adhere to policy requirements at school level, with regions providing oversight and support where required.

6.4 Group and Regional Legal Teams

6.4.1 Support the development and maintenance of the Group's data classification taxonomy to ensure alignment with applicable legal and regulatory requirements.
6.4.2 Provide guidance on compliance with data protection and information security laws and regulations, including support during security incidents or breaches.
6.4.3 Collaborate with Group Cyber Security and IT teams to identify and address legal risks related to the protection of data and information systems.
6.4.4 Advise on the legal implications of regional and group level security policies, controls, and incidents.

6.5 Employees

6.5.1 Comply with the Group Information Security Policy and associated procedures.

6.5.2 Protect organisational information and report any suspected security incidents promptly.

6.5.3 Complete mandatory security awareness training and apply best practices in day-to-day activities.