Information Security Policy

Contents

1. Document Control

Version Control

Date	Version	Changes	Author

16/06/2021	0.01	First draft of policy incorporating current employment contract clauses	Information Security Team
22/06/2021	1.0	Approved for publication by the IT Director	Information Security Team
20/06/2022	2.0	Policy reviewed and minor amendments made. Objectives remain as previous.	Information Security Team
21/06/2023	3.0	Policy reviewed and objectives updated. Also included reference to this policy being available on Jobs 22 website.	Information Security Team
25/06/2024	4.0	Minor amendments made to purpose of policy and added reference to transition and maintenance of ISO27001:2022	Information Security Team
13/11/2024	5.0	Minor amendment made to reference Healthfind. Addition of new Annex 1 and Annex 2.	Information Security Team
13/05/2025	6.0	Minor amendments made to capture applicability to AKG Learning and remove specific reference to Healthfind.	Information Security Manager
09/04/2026	7.0	Minor amendments to include applicability to ITS and remove reference to transition to 2022 ISO27001 Standard	Information Security Manager

A current version of this policy document is available to staff on the AKG Hub.

Policy Owner

This policy is owned by the UK Country Manager.

Policy Scope

AKG Employment	AKG Learning	AKG Health	Intuitive Thinking Skills
Yes	**Yes**	**Yes**	**Yes**

Any variations in the policy relating to those entities in scope will be clearly articulated in the policy. Otherwise, the policy applies equally to all entities in scope.

Where an entity is out of scope, they will have their own policy in place available within the policy store.

This policy applies to all employees with access to any company information asset.

Document Review Arrangements

The Information Security Policy will be reviewed at least annually.

Next Review Date:	08/04/2027

2. Introduction and policy overview

- To communicate the Leadership's commitment to protecting the confidentiality, integrity and availability of the organisations' information assets.
- To set out the strategic direction for the management of information security.
- To serve as the overarching policy from which the framework of policies, procedures, and records that form the ISMS derive.
- To set out the organisations' information security objectives.

Policy Statement

We are committed to protecting the confidentiality, integrity and availability of our information assets. It is of paramount importance that we ensure the privacy, accuracy and security of the personal data we collect, process, and store in the course of delivering our services. Notwithstanding our legal obligations, we understand that safeguarding personal data is a foundation of the trust placed in us by our participants, service users, learners, staff, partners, and our delivery commissioners.

Signed:

Andre Simm
IT Director

3. Responsibilities

- Department Heads are committed to ensuring all information assets held, stored or processed, including those processed on by a third party, are securely protected against unauthorised access, disclosure, alteration or loss in accordance with legal, regulatory and contractual obligations.
- Information security management and processes are aligned with and support the aims and objectives set out in strategic business plans. Information related risks will be identified, assessed and mitigated through risk assessments, risk treatment plans and a register of security controls known as the Statement of Applicability.
- The organisations commitment to, and management of, information security is governed by the Information Security Steering Group (ISSG) which meets quarterly. The ISSG is chaired by the IT Director, and the Group provides overarching governance for information security and data protection and comprises senior management representatives. The UK Country Manager may be invited to attend on an annual basis.
- The UK Country Manager acts as the Senior Information Risk Owner but has delegated his responsibilities as SIRO to the Business Intelligence Director, with the exception of Board representation.

4. Objectives

1. To successfully maintain ISO27001:2022 Certification.
2. To demonstrate continual improvement by the ongoing evaluation and review of effectiveness measurements and addressing identified areas for improvement.
3. To take account of feedback from interested parties to support the drive for continual improvement.
4. To maintain Cyber Essentials and Cyber Essentials Plus Certification.
5. To ensure the organisation fulfils its legal, regulatory and contractual responsibilities under Data Protection and other relevant Legislation and contractual requirements.
6. To ensure information security is embedded throughout the organisation and is taken account of in all established management frameworks, strategic aims and objectives and organisational process and practice.

7. To preserve the confidentiality, integrity and availability of all information assets. This will be achieved by:
    a. Determining and documenting the processes into which information security should be integrated across all functions of the organisation.
    b. Ensuring that all users who access the organisation's ICT systems and/or premises are aware of their security responsibilities.
    c. Ensuring that all information and associated assets are accessible to authorised users when required and that information is only accessible to those authorised and to prevent unauthorised access to company information, intellectual property and information processing assets.
    d. Ensuring that safeguards are in place to protect the accuracy and completeness of information and to prevent deliberate or accidental, partial or complete, destruction or unauthorised modification of data or any other information asset.
8. To ensure a risk-based approach underpins all strategic decision making and that privacy and information security issues and risks are identified, assessed and managed as part of this decision-making process.
9. To ensure the organisation implements and maintains a fully integrated records management process which meets its legal and contractual obligations and assigns responsibility for facilitating the timely disposal/deletion of all records.
10. To ensure performance against these objectives' forms part of the Effectiveness Measurement monitoring by the ISSG.

Signed by:

Ayden Sims, UK Country Manager

Date: 09/04/2026

Annex 1: AKG Values Matrix

Purpose of the AKG Values Matrix

We are committed to ensuring everything we do and every decision we make is aligned to our core values. This short matrix ensures that all our policies are developed to align to and support our core values.

Policy	Information Security Policy
Matrix completed by:	Information Security Manager
Date of assessment:	09/04/2026

Assessment

AKG UK Value	Summary of how the policy aligns to and supports our values.
Empowerment	Empowering all staff, regardless of their role, to take responsibility for the secure protection of information assets
Empathy	All staff, regardless of their role, can work together to demonstrate the organisation's commitment to information security
Integrity	The policy outlines at high level the measures in place to preserve the confidentiality, availability and integrity of all information assets
Connected	This policy seeks to foster a culture of information security and data protection awareness across all entities within AKG UK

Annex 2: Equality Impact Assessment

We are committed to promoting the quality of opportunity for all our staff and service users, and for ensuring our staff and beneficiaries do not feel discriminated against, harassed or victimized by our working practices, whether or not they share a protected characteristic. With this in mind, allowances can and will be made wherever reasonable and practicable to any of the rules and conditions outlined within this policy if it is determined that any individual or group is negatively impacted by one or more of the rules and conditions outlined in it.

If you feel this policy is discriminatory in any way, or that your personal circumstances are such that adjustments to the conditions of the policy are required for you, then you are encouraged to speak with your line manager at the earliest opportunity, or to contact the policy owner. Any issues raised will be treated without prejudice and in the strictest confidence.

Purpose of an Equality Impact Assessment

An Equality Impact Assessment is a tool for identifying whether or not strategies, projects, services, guidance documents, working practices or policies have an adverse or positive impact on a particular group of people or equality group so that any necessary adjustments can be made to mitigate those adverse impacts, or to further promote those positive impacts.

While only public bodies are legally required to complete Equality Impact Assessments, we have adopted the process in line with our own commitment to quality and diversity and as part of our continual improvement efforts.

This Equality Impact Assessment is for:	Information Security Policy	
Completed by:	Information Security Manager	
Date of assessment:	09/04/2026	
Objective:	To ensure that the implications and potential impact, positive and negative, of the Information Security Policy for all staff have been fully considered and addressed, whether or not the staff members share a protected characteristic	

Assessment

Equality Area	Positive	Neutral	Negative	Summary
Age	☐	☒	☐	
Disability	☐	☒	☐	
Pregnancy or maternity / paternity	☐	☒	☐	
Race and ethnicity	☐	☒	☐	
Gender	☐	☒	☐	
Sexual orientation	☐	☒	☐	

Negative Impacts and mitigations

Negative Impact	Mitigation	Owner
None		