SHREWSBURY COLLEGES GROUP

INFORMATION GOVERNANCE POLICY

1. Purpose

Establish the overarching structure for, and consistent approach to, information governance across Shrewsbury Colleges Group.

Ensure that clearly defined roles and responsibilities are identified for key individuals and teams, designed to set out the minimum protocols required across the College.

Develop and embed professional and appropriate behaviours when handling information and build trust with students and other key stakeholders.

2. Scope

This policy intends to be consistent with all applicable legal and regulatory compliance requirements including, but not limited to, Principle 7 of the Data Protection Act (2018), the Accountability and Governance aspects of the General Data Protection Regulations (2018) and Freedom of Information Act (2000).

3. Policy statement

It is the policy of Shrewsbury Colleges Group to have a robust, consistent and effective approach to information governance and to ensure that protocols and procedures are in place covering related IT resilience, professional conduct, and trust building activity.

The policy will facilitate the establishment of a holistic management process for information governance. It will set out how the College community will be made aware of the risks related to information handling and processing and develops an ability to prevent and respond to potentially disruptive events related to information governance, protecting the interests of students, employees, parents, employers, and the College's brand.

Implementation of this policy complements the General Data Protection, Data Retention, Data Breach, and Cyber Security policies by establishing who is responsible and accountable for their implementation. It complements the Risk Register and Board Assurance Framework policy by providing a means of discovering, assessing, reporting and treating risks related to information governance.

4. Policy Detail

Data Protection Officer (DPO)

Shrewsbury Colleges Group is required to nominate a Data Protection Officer because it is defined as a Public Authority under the definition within the Freedom of Information Act.

The DPO is responsible for:

- Reporting to the highest level of management
- Monitoring of the organisation's compliance with GDPR, privacy laws, and policies
- Record keeping

- Advising colleagues, training and awareness raising
- Advice regarding Data Protection Impact Assessments
- Facilitating or carrying out audits
- Support following a data breach
- Liaise with ICO on all matters regarding a breach

Required skills include:

- Indepth understanding of GDPR and other data protection laws and practices
- Knowledgable about the organisation, including processing operations
- Accessible to students, staff, governors, employers and ICO

After due consideration of the roles and skills required, and the complexity of data and systems within the College, the Vice Principal – Quality, Apprenticeships, and Information has been designated as the DPO.

The college's Board will receive annual reports from the DPO covering key policy and procedural compliance, high-level data breach summary, and overview of staff training activities. The Audit Committee has decided to include GDPR compliance within the College's independent internal audit cycle. Should an individual have concerns that a conflict of interest results in a data breach, the college's Whistle Blowing Policy can be used to raise their concerns with the Board.

Responsibilities

The **Senior Leadership Team (SLT)** is responsible for:

Establishing the necessary resource and processes in each department to be able to respond to the changing needs of information governance.

Informing line managers in departments of the gaps in current practice, emerging threats and vulnerabilities, opportunities and the front line information governance realities for students and key stakeholders.

Developing an organisational capability that brings coherence to information governance and ensures the College is able to manage any disruption, complexity and/or change.

Each member of the **Senior Leadership Team (SLT)** will be responsible for ensuring the active support of effective information governance practices within every department across the College, and at every campus.

Whenever there is a significant change in the operating environment or a practice or procedure, the SLT member must identify and review this with their department, assisted by the DPO. The DPO will advise regarding the identification, classification, and specification of solutions that are achievable and consistent with the wider College information governance approach.

Accountability

The SLT are accountable to the Principal for the maintenance of effecive Information Governance processes.

The DPO is responsible for maintenance of the policy and circulation to relevant parties.

The DPO and Head of Technical Services are responsible and accountable for the appropriateness of the protocols, the practices and procedures intended to support Information Security Management.

SLT must approve this policy and any changes to it.

Employees are accountable and responsible for their own actions with regards to information governance, which is supported by the IT Acceptible Use Policy.

All managers are accountable and responsible for ensuring that the policy is effectively applied and adhered to at all times.

Those providing services directly to students will instruct them on good information governance where they need to ensure appropriate management of data and resources, for example through the College IT Acceptable Use Policy.

Information and communication

This policy and any updates to it are accessible on the College intranet; InfoPoint.

Training for this policy will be included within all staff induction activities. Ongoing staff training is delivered via online data protection included within the college training plan.

Policy monitoring and maintenance

The DPO is responsible for monitoring adherence to and effectiveness of this policy.

All instances of internal control risks and/or non-compliance with the policy must be reported to the DPO, in the first instance, and will be reported to SLT where appropriate.