Senior Information Risk Owner (SIRO) Responsibilities

Role Title: Senior Information Risk Owner
Grade: Head Teacher
Lead: Mrs Manookian

- The role of the Senior Information Risk Owner (SIRO) was created to provide board-level accountability and greater assurance that information risks are addressed. The SIRO ensures that information risks are treated as a priority for business outcomes. The SIRO also plays a vital role in getting their organisation to recognise the value of its information enabling them to use it effectively.

- The SIRO as an executive-level champion: Information assets are integral to the functioning of any modern business and essential to delivering corporate objectives. By understanding, addressing and capitalising on the risks and facing an organisation's information assets, a SIRO can ensure services are delivered efficiently and with greater value for money.

- The SIRO as a champion of governance: The SIRO role is an integral part of any organisation's Information Governance Framework. As the SIRO is accountable to the Executive for risks they should actively work with relevant experts and other organisations to determine the most effective and proportionate information control measures.

- The SIRO as a champion for cultural change: The SIRO plays a pivotal role in championing a culture which is resilient, adaptable and open to change in order to effectively deliver business priorities.

Data Protection Lead (DPL)

Role Title: Data Protection Lead
Grade: Manager
Lead: Mrs Tory-Hill

The Data Protection Lead (DPL) in schools acts as a point of contact between the school and the Data Protection Officer (DPO). They must ensure staff are aware of their responsibilities in relation to data protection. They will work closely with the Senior Information Risk Officer (SIRO), who is usually the Head Teacher. The role is typically filled by a central office role such as school business manager, finance manager etc, or a deputy head teacher, though it is often undertaken by the SIRO themselves. It is for the school to determine who is nominated.

Data Protection Officer (DPO)

Role Title: Data Protection Officer
Lead: IGS

Oversight & Approval of:

Advice & Guidance:

The DPO should be sufficiently knowledgeable in Data Protection law to provide correct guidance on the legal requirements of processing personal data to employees and data processors for which the organisation is responsible

Records of Processing Activity:

The DPO should be monitoring the process of reviewing the Organisation's Records of Processing Activity, which documents compliance with the Data Protection Act, in order to approve its completeness, currency and accuracy

Compliance Reporting:

The DPO should be satisfied with the scope of reporting on Data Protection compliance metrics, its frequency, its accuracy, and that the receiving audience is appropriate and gives the report sufficient weight. The DPO should provide commentary on reports so that senior leaders can receive qualified opinion on whether the Organisation is compliant

Performance Auditing:

The DPO should be satisfied that there is appropriate testing of the Organisation's compliance activities, its frequency and that there is either a satisfactory outcome or that action points are identified as part of improvement plans to which senior leaders give sufficient support.

Data Breaches:

The DPO should be assured that data breaches are being correctly identified, reported, investigated and recorded effectively. The DPO should advise the Organisation on whether a particular breach meets the criteria for reporting to the ICO, and with the Senior Information Risk Owner's (SIRO) agreement, managing the ICO reporting process within the statutory timescale.

Impact Assessments:

The DPO should ensure that where activities which require a statutory Data Protection Impact Assessment, this is undertaken. Where an assessment is undertaken, the DPO must approve that the proposed processing of personal data is compliant with the law.

Risk Management:

The DPO should monitor the Organisation's risk review process to ensure those risks which impact on Data Protection compliance are appropriately reviewed and the DPO has the opportunity to comment on and approve the identified mitigations.

Information Sharing:

The DPO should ensure that employees have clear guidelines to follow on when it is appropriate to share personal data and how this should be done securely. Where new requirements to regularly share data are identified, the DPO should arrange for Information Sharing Protocols to be approved before the activity commences.

Statutory Requests:

The DPO should be satisfied that the Organisation has in place effective processes for recognising considering and responding to statutory requests relating to the Data Subject rights under Data Protection law.

Complaints:

The DPO should be satisfied that the Organisation has in place effective processes to identify and manage complaints made regarding the processing of personal data from both members of the public and the ICO.

Policy:

The DPO should ensure that all policies which relate to the processing of personal data are legally compliant, reviewed at an appropriate frequency, approved with DPO guidance by senior leaders, and that they are accessible to appropriate audiences.

Training:

The DPO should be satisfied that employees receive appropriate training in the Organisation's data processing policies and procedures according to their roles and responsibilities. Relevant training activities and awareness communications should be recorded and approved by the DPO.

Registration:

The DPO should be satisfied that there is an effective process in place for registering the Organisation's details with the ICO, reviewing this annually, paying the annual fee to the ICO and renewing when the registration expires.