Grays Convent

HIGH SCHOOL

DPO ROLE PROFILE & RESPONSIBILITIES

Defined responsibilities of the DPO to be used in addition to an existing substantive role profile

Approved by	Information Governance Board (IGB) of Finance Health & Safety Committee of Grays Convent High School
Date Approved	Spring 2018
Version	1
Review Date	Spring 2019 or as there are changes in legislation

Our Mission Statement

At Grays Convent we recognise the value of each individual as a gift from God to the world. We are a Catholic school founded by the La Sainte Union Sisters and our ethos is one of unity, prayer, worship, service and work. We strive to follow the example of the Sacred Hearts of Jesus and Mary by enabling learning to take place in a caring and accepting community. We are blessed by Jesus the Good Shepherd, try to follow him in everything that we do, and in doing so make the most of our God given talents. We are one with God.

Job Profile

Role Title: Data Protection Officer Lauri Almond

The Role:

This role is aligned to the implementation of the requirements of one of the biggest changes to Information Laws since the introduction of Freedom of Information Laws in 2000. The General Data Protection Regulation (2016) (GDPR) requires entities that process Personal Data to have a series of controls and processes in place. One of these requirements, as outlined in Articles 37-39 of the Regulation, is to have a defined Data Protection Officer for the organisation.

The Data Protection Officer will be responsible for advising and monitoring the business's compliance with the GDPR, including performance of other formal duties as defined by the GDPR.

The Data Protection Officer applies knowledge and experience to assist the organisation in delivering services to both internal and external customers.

Key Accountabilities:

- Working with the organisation to ensure compliance with their obligations under the General Data Protection Regulation and any relevant UK legislation;

- Working with organisation to monitor compliance with the Regulation, with relevant supporting UK legislation and with relevant organisational policies in relation to the protection of personal data.

- Report on the status of compliance with the Regulation to the Leadership Team and other stakeholder scrutiny groups, including briefing on specific matters for their review.

- Working with the organisation to oversee and assist in staff awareness-raising and training both online and face to face where required.

- Acting as a key stakeholder for any and all Data Protection related audits and compliance reviews, completed both internally and externally.

- Working with the organisation to provide advice and review of data protection impact assessments where required and monitoring their ongoing implementation and review. This includes acting as the formal sign off of any assessments meeting the criteria.

- Working with the organisation to investigate and process adverse incidents ensuring that any incidents that require notification to the Data Subject and/ or Supervisory Authority are completed within the 72 hour timeframe.

- Working with the organisation to advise on any Information Sharing Protocols looking to be established and shared as part of the organisation's membership of the Whole Essex Information Sharing Framework (WEISF).

- Cooperate with the Supervisory Authority (currently the Information Commissioner's Office).

- Act as the contact point for the supervisory authority on issues relating to the organisation processing of Personal Data and compliance with the GDPR and working with the organisation to resolve these.

- Act as the contact point for data subjects on issues and queries relating to the organisation's processing of Personal Data and compliance with the GDPR and working with the organisation to resolve these.

- Lead on any prior consultation needed with the supervisory authority for any organisational processing of Personal Data where required and to support the organisation and supervisory authority in this process.

- Liaise with the Leadership Team regarding Data Protection & any other information governance matters.

- Develop and maintain own skills and expertise to keep up with current requirements of the Regulation and supporting legislation.

- Build strong relationships with other Data Protection Officers to encourage the sharing of knowledge, best practice and reliable information sharing arrangements.

Knowledge, skills & experience:

- Strong knowledge of Data Protection legislation, specifically the General Data Protection Regulation 2016 and any supporting legislation.

- Practical knowledge of Data Protection compliance including best practice.

- Experience working with Data Protection in the Public Sector or experience working with complex legal matters and being able to decipher them simply for other audiences.

- Relevant qualifications in Data Protection Law and/or Information Law / Information Governance that covers the General Data Protection Regulation 2016.

- Understanding of Information Risk Management including horizon scanning for emerging risks, reporting and analysis and route cause analysis.

- Good communication and interpersonal skills in order to liaise with staff at all levels, including Board level, and build lasting and productive relationships with internal and external stakeholders.

Data Protection Officer Responsibilities

Named Contact for Data Subject Complaints
Data Protection Officer Lauri Almond, at IGS@essex.gov.uk or by calling 03330 322970

Single point of contact for the regulator (ICO)
P Johnson, Headteacher & SIRO

Oversight & Approval of:

- Advice & Guidance
- Records of Processing Activity
- Compliance Reporting
- Performance Auditing
- Security Incidents
- Impact Assessments
- Risk Management
- Information Sharing
- Statutory Requests
- Complaints (Direct & ICO)
- Policy
- Training
- Registration

Named Contact for Data Subject Complaints

The DPO's name and work contact details should be published in order for Data Subjects to direct their enquiries and complaints.

Single point of contact for the regulator (ICO)

Where there is involvement with the ICO, the DPO should act as the single point of contact to ensure that correspondence is well managed, approved and within timescales.

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.

Security Incidents:
The DPO should be assured that security incidents are being correctly identified, reported, investigated and recorded effectively. The DPO should advise the Organisation on whether a particular incident meets the criteria for reporting to the ICO, and with the SIRO's 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 be the role to 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.