TARGET OPERATING MODEL FOR INFORMATION GOVERNANCE

SCOPE

This "Target Operating Model" relates to how the Robert Gordon University ensures compliance with the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA).

The university is a single campus higher education institution providing education to both undergraduate students and post graduate students. The university attracts students and staff from both the UK and international markets and provides education to both on campus students and off campus students by distant learning. The university also engages in various research activities.

The university requires to processes personal data to allow it to function as described above. The university's only campus is situated in Aberdeen on the north east coast of Scotland therefore the supervisory body to which the university reports is the UK Information Commissioner. The university is registered with the Information Commissioners Office (Registered number Z5607918)

ROLES and RESPONSIBILITIES

The role of the Data Controller for the university is held by the Director of Planning and Policy. The Data Controller has overall responsibility for ensuring that the university process personal data in accordance with GDPR and the DPA. The Data Controller reports directly to the Principal.

The role of the Data Protection Officer (DPO) is held by the Information Governance and Complaints Officer. The Data Protection Officer is responsible for the day to day compliance of GDPR and DPA. The role requires that the Data Protection Officer is the single point of contact between the university and the Information Commissioner. The DPO ensures compliance through developing policy and guidance, delivering training and awareness, monitoring processing activities, conducting privacy impact assessments, investigating data breaches and providing advice where appropriate. In the appropriate circumstances the DPO may raise a data protection matter directly with the university's Principal and Vice Chancellor.

The university has 12 schools (including a graduate school) and 20 administration and support departments. Each school or department has a designated Data Protection Champion. These champions have received enhanced training in data protection and are the single point of contact for each school or department for data protection related matters. They assist the DPO when a data breach has occurred, provide support when a data subject access request has been made. They also can provide basic data protection advice to their respective school or department.

Each member of staff at the university completes a mandatory data protection training module as part of their induction. Every member of staff have an obligation to ensure they are complaint with the relevant data protection legislation. As part of the university's preparations for GDPR every member of staff was required to attend a one hour training session.

POLICIES and PROCEDURES

The university has a record of all its processing activities which is available on its website. It also has a range of information governance policies and procedures, which can be found by following the link below and include policies specific to data protection. these are available on the university website to staff, students and the general public and provide staff with guidance on matters such as general information about compliance with GDPR, what to do if somebody makes a data subject access request, what do in the event of a data breach and how to report it, when and how to conduct a data privacy impact assessment, the university's use of CCTV and the contact details for the Data Protection Officer.

The following policy and guidance can be found on the policy page of the university's website at the link below:

- Guide to Information Governance
- Information Governance Policy
- Policy for use of IT facilities
- Detailed guidance for the use of IT facilities

https://www3.rgu.ac.uk/about/planning-and-policy/information-governance/information-governance

A data subject can locate the contact details for the Data Controller and the Data Protection Officer, access privacy statements, about their rights, in relation to data protection, and how to make a complaint if they believe their rights have been breached.

A Risk and Controls Matrix has also been developed and forms annex to this operating model.

TRAINING and CHANGE MANAGEMENT

The DPO scans the external environment for information relating to information governance which may impact on the university. This is done through membership of various groups and online forums such as the Scottish Higher Education Information Practitioners' Group (SHEIP), the ICO's website and attendance at conferences, meetings, lessons learned from data breach investigations and attending training courses.

The DPO will be responsible for disseminating any new information or change identified to the relevant staff at the university using a variety of media e.g. all staff bulletin, training sessions, the DPO is also responsible for ensuring that any changes that are required to be made to policy and guidance are carried out.

Every new member of staff employed at the university must complete a mandatory online training module as part of an induction process. Each Data Protection Champion will be invited to regular training sessions conducted by the DPO to ensure their knowledge and practice in their respective area is in line with current practice.

TOOLS and INFRASTRUCTURE

The majority of personal data processed across the university is carried out using various software programs hosted on the university's IT infrastructure. Personal data must not

be processed via third party cloud services such as dropbox, google docs. Staff must adhere to the relevant IT use policies found at https://www3.rgu.ac.uk/about/planning-and-policy/policies/policies/ .
The development of new, or the amendment of existing, systems which process personal data must undergo a Privacy Impact Assessment (PIA) screening exercise to establish whether or not a full PIA is required. The DPO assists with this process.
The university's IT Department is responsible for maintaining and updating the security of the IT infrastructure. Any personal data which is processed in manual filing systems must be done using appropriate physical security.

COSTING
The duties carried out by the Data Controller and Data Protection Champion in relation to data protection are peripheral to main roles carried out by these members of staff therefore there are no precise costs attributed to data protection. The role of DPO is full time and the salary costs are met by the Strategy, Planning and Policy Department of the university.
Personal development of the DPO and training sessions for the data protection champions are met by the Planning and Policy Department.
Costs associated with IT security and maintenance are met by the IT Department budgets.

FEEDBACK, REVIEW and CONTINUOUS IMPROVEMENTS
All schools and departments have conducted an audit of all data they hold and the processing activities they undertake. All schools and departments are required to conduct an annual review of the data and activities and provide an update to the DPO.

The DPO conducts an annual review of the record of processing and the risk and control matrix and implement any identified changes required. Lessons learned from data protection breach investigations, data subject requests and from best practice adopted across the higher education sector. Improvements and changes identified will be feedback to employees through data champions by the DPO and reported to senior management on a quarterly and annual basis.