Role Profile

Role title: Data Protection Lead

Reports to: Chief Operating Officer

Job purpose: The main purpose of this role is to promote BACP's adherence and compliance with the provisions of the Data Protection Act/GDPR and achieve the highest standards of information security for BACP.

Financial: TBC

Staff: 0 Direct and 0 Indirect

Other: N/A

Principal accountabilities:

1. Act as BACP's Data Protection Officer (DPO) as defined by prevailing data protection legislation to monitor and ensure the organisation's compliance with that legislation.
2. Be the first point of contact for enquiries from staff on data protection matters including Subject Access Requests (SARs), providing them with comprehensive advice and guidance and rights to be forgotten
3. Coordinate all data subject communications, including Data Privacy Statements, to ensure data subjects are aware how their data is used, their rights under current data protection legislation and the timely conclusion of the same to ensure BACP complies with best practice.
4. Act as the point of contact for all data breaches and maintain the data breach and near miss register, ensuring that lessons are learned, and any breaches are reported to the ICO within the legislation.
5. Engage with internal teams to ensure the necessary Data Protection Impact Assessments (DPIA) are completed and any risks are identified, and the consequential requirements are appropriately considered at the relevant times and any conclusions and actions are documented.
6. Advise BACP on security concerns and recommendations with regard to the security of data and systems and to build strong relationships with all departments in order to foster excellent team working and support for improved data security management.
7. To conduct routine data protection audits and co-ordinate ongoing learning across staff and volunteers. To ensure reducing data footprints and data anonymisation programmes are continuously improved.
8. To support members with regard to data protection queries and questions relating to their own practice
9. Report on information security incidents, and present data protection reports to BACP's trustees as necessary.

10. To assist and support the management of security with particular reference to shared information systems, website privacy compliance and IT infrastructures.
11. Define, document and implement security policies for the organisation, working to develop the ICT Security Policy Framework.
12. Undertake an annual health check of all BACP's infrastructure systems and facilities, to include a network & vulnerability analysis with summary report of recommendations for improvement.
13. Undertake any training activity to ensure BACP's policies and procedures are understood, and to develop any new knowledge within the role.
14. Adherence to standards/best practices, such as ISO 27001 and Information Technology and Infrastructure Library (ITIL).

BACP Principal accountabilities

- To be a BACP ambassador by upholding and demonstrating our values at every opportunity, through verbal, written and face to face communication.

Context:

Operating environment: Across the organisation for any data protection and information security matters / GDPR.

Framework & boundaries: Data protection policy needs to adhere to external standards, best practices and current legislation, such as the DPA 1998/2018 including GDPR.

Organisation:

Relationships:

Direct reports: None

Manager: Chief Operating Officer. Monthly 121s, support and guidance when required

Other contacts: All levels of staff.

Knowledge & experience:

Education: Educated to degree level or substantial senior technical experience.

Experience: Working in a senior expert role within a local authority or membership organisation at corporate level.

Competencies:

- Expert knowledge and practical experience of data protection law, to include the Data Protection Act and GDPR.
- High-level of IT literacy with direct experience of working with data security applications, systems and solutions.

- Competence to drive forward change effectively, using a flexible, consultative and supportive approach.
- Ability to get things done without direct authority over a team. Good negotiating and influencing skills. Capable of communicating effectively at all levels in both written and oral presentation.
- Proven experience in dealing with all aspects of the Data Protection Act, including handling breaches, SAR's, policies and risk management.
- Previous experience and evidence of undertaking data security checks
- Experience of working to standards such as ISO 270001 and Information Technology and Infrastructure Library (ITIL) and an awareness of the latest developments and innovations in data security.
- Excellent time management skills to work effectively under pressure.
- A solid understanding of good project delivery and case management so that objectives are achieved to deadline and within budget.
- High-level of discretion when dealing with confidential and/or sensitive issues and information.
- Skills required to analyse complex issues and data, including research, financial and management information, both verbally and in writing.
- Ability to undertake research and development work to have a strong awareness of the latest developments and innovations in data security management. To ensure the organisation has suitable compliancy management tools in place.
- Experience of providing training and guidance around data security issues, to staff with varying abilities.
- Ability to work flexibly and on occasions out of office hours.

Job challenge: TBC

Additional information

TBC