



Job Title (Location)	Information Security and Compliance Officer (London Hammersmith or Glasgow)
Salary and Band	Band 6 (core salary of £33,535 to £44,911 plus London Weighting of £6,707 to £8,164 only applicable in London)
Annual Leave	27 days plus 9 Bank Holidays for full-time hours
Reports to	Head of IT
Direct Reports	N/A

About Maggie's

We provide free cancer support and information in our specially designed centres across the UK and online. Working alongside NHS hospitals, Maggie's centres are staffed by expert Cancer Support Specialists, Psychologists and Benefits Advisors, helping people to take back control when cancer turns life upside down.

Our long-term ambition is to be there for everyone with cancer in the UK at all 60 cancer centre sites to ensure that there is no-one living with cancer who is unable to access the expert psychological and information support that they so desperately need to live the best quality of life possible. The next five years brings us over the halfway mark to achieving this goal.

About the Post Holder

You will have at least 24 to 36 months in a similar role and be educated to degree level. Certified in the relevant security qualifications (CISSP, CISM or working toward), you will have experience with both local and wide area networks and an understanding of the relevant network protocols, intrusion detection / prevention, anti-virus and patching applications on both user end point and server.

Working with the Head of IT and Data Protection Officer (DPO) you will ensure that all Maggie's systems, and data are secure and GDPR compliant. You must be able to communicate at all levels, translating security concepts into plain English, verbally and in writing, and be able to work with sensitivity to the environment where visitors are receiving emotional support.

About the Role

Reporting to the Head of IT, the role will require in-depth understanding of information security, technology architecture and business security. The Information Security and Compliance Officer will be responsible for maintaining Information Security policies and controls, in addition to application, infrastructure and network security reviews to ensure the security of all Information Security assets

at Maggie's.

The Information Security and Compliance Officer will be involved with the prevention, identification and detection of IT and information security risks over the entire organisational environment, whilst supporting Maggie's operations and key processes. Infrequent UK wide travel and un-social hours working will be required in this role.

Key Responsibilities

- Work closely with the Head of IT and Data Protection Officer to ensure that appropriate security guidance is provided to support IT or other Maggie's departmental projects.
- Input in to the design and implementation of standards, policies, guidelines and appropriate architectural principles to ensure the Maggie's cyber security goals continue to be met.
- Take ownership and ensure Governance, Policy and Procedures in relation to Management of Information Security meets agreed standards within Maggie's.
- Develop and implement various DLP policies for our data.
- Ensure Maggie's has as an effective data retention, classification and archiving process in place.
- Support the DPO with any reported data breach incidents and assist with any subject access request related tasks.
- Audit any external platforms that will be used by Maggie's to ensure they meet our security standards.
- Head our Cyber Security Incident Response team.
- Assist with any external audits of Maggie's core platforms and infrastructure.
- Respond to enquiries from staff and provide security advice as required.
- Promote cyber security awareness within the organisation.
- Coordinate internal Phishing campaigns to maintain staff security awareness.
- Perform internal security and user permissions audits.
- Lead on organising penetration testing and ensuring any corrective or remedial work is completed as a result.
- Ensure our core platforms and network infrastructure are securely configured.
- Monitor our core platforms and systems for any unusual activity, including insider threats.
- Monitor the threat landscape and the potential impact on Maggie's

Essential skills and experience

- Educated to degree level.
- Certified to either CISSP or CISM level or working towards.
- A good understanding of IT networking (including firewalls and protocols) and access management concepts.
- Broad knowledge of a wide range of Information Technology systems including cloud computing platforms (especially Microsoft 365 and Azure) with a deep understanding of the inherent security risks associated with these technologies.
- Experience working with and deploying SIEM and CASB systems.
- Intrusion detection / prevention experience.
- Experience of Microsoft conditional access policies advantageous.
- Understanding of information security principles and best practice (e.g., ISO27001 and ISF Standards of Good Practice for Information Security).
- Understanding of, and practical experience of applying the General Data Protection Regulation (GDPR), the Freedom of Information Act and other related legislation, standards and codes of practice.
- Ability to present security topics to a non-technical audience and presenting the business value of security.
- Ability to communicate business and technical risk to all levels of audience.
- Excellent interpersonal skills with the ability to build and influence teams; and self-motivated.