

Summary

Job title	Cyber Security Education & Awareness Manager
Division	University Administration and Services (UAS)
Department	Cyber Security, Digital and Information Services
Location	Central Oxford Hybrid working possible (minimum 2 days onsite per week)
Grade and salary	Grade 8: £49,119-£58,265 per annum
Hours	Full-time 37.5 hours per week Whilst this is a full-time post, we welcome applications from candidates who wish to work part-time (minimum 30 hours/0.8 FTE) and/or flexibly
Contract type	Fixed-term (to 31/07/2029), with the expectation of extension, subject to funding
Reporting to	Cyber Security Programme & Culture Director
Vacancy reference	189311
Additional information	Applications on a secondment basis will be considered for eligible internal candidates. Any approved secondment would be limited to the duration of the post or a maximum of three years in exceptional circumstances, in line with University secondment guidelines .

The role

The University of Oxford has embarked on an ambitious Cyber Security Improvement Programme to strengthen cyber security across the collegiate University. Education, awareness and positive security behaviours are an important part of this work, helping staff and students understand cyber risks and take practical steps to protect themselves and the University.

The Cyber Security Education & Awareness Manager will lead and have operational responsibility for the University's cyber security education and awareness function, setting its approach and priorities and developing



and delivering a University-wide programme designed to reduce human-related cyber risk and strengthen security culture across approximately 24,000 staff and 20,000 students.

Working closely with colleagues across Cyber Security, Digital and Information Services and the wider University, the post holder will translate cyber security risks, requirements and technical information into effective communications, training and engagement activities for both technical and non-technical audiences.

The role will lead the development and delivery of the University's cyber security education and awareness programme, determining priorities across training, campaigns, phishing awareness, communications and stakeholder engagement. The postholder will use cyber risk, behavioural and engagement data to evaluate impact, identify emerging priorities and determine improvements to the University's approach.

The postholder will use specialist expertise, cyber risk intelligence and behavioural evidence to determine priorities, advise Cyber Security leadership and governance groups, and develop appropriate interventions in response to changing threats, risks and organisational priorities.

Through effective communication, stakeholder engagement and continuous improvement, the role will help embed cyber security into everyday working practices and contribute to the University's long-term security posture.

Flexible working

Working arrangements

IT Services and DGU support a hybrid working model. Most staff are expected to spend part of each week on site (typically 2–3 days) to collaborate with colleagues, participate in team activities, and engage with users and stakeholders. Some roles with high levels of user interaction, operational requirements or training responsibility may require more frequent on-site presence. Specific patterns will be agreed within each team to balance flexibility, inclusion, and service delivery.

About our Service Delivery Model

IT Services and the Digital Governance Unit are implementing a new service delivery model as part of the University's wider digital transformation. This model focuses on continuous improvement, user-centred design, and empowered multidisciplinary teams that deliver measurable value to the University community. The change moves us away from time-limited project delivery towards ongoing enhancement of digital services across Portfolios and Service Streams. Teams work collaboratively within agile frameworks, balancing flexibility with consistency through agreed guardrails. This approach supports professional development, fosters collaboration, and strengthens the link between day-to-day work and the University's research and education mission.

All staff are expected to support the department's continuous improvement culture by engaging with relevant training, contributing to communities of practice, and promoting inclusive, collaborative working. As our service delivery model evolves, roles may adapt to reflect emerging technologies, processes, and user needs.

Core values

All staff are expected to demonstrate behaviours that reflect our departmental values – People, Excellence, Partnership, Service, and Sustainability. This means valuing colleagues and users, striving for continuous improvement, collaborating across teams, delivering reliable and user-focused services, and making responsible, sustainable decisions. Staff should act openly, supportively, collaboratively, accountably, and respectfully, contributing to a culture of belonging and feedback.

Responsibilities

- Develop, gain agreement for and lead implementation of the University's cyber security education, awareness and behaviour-change strategy and roadmap, ensuring alignment with University cyber security strategy, the Cyber Security Improvement Programme and institutional priorities.
- Hold operational responsibility for the University's cyber security education and awareness programme, setting priorities and overseeing the delivery of training, campaigns, communications, engagement and behaviour-change interventions across the collegiate University. Utilising platforms including MetaCompliance, SharePoint and Teams.
- Manage and coordinate phishing awareness and simulation activities, analysing results and using findings to identify behavioural risks, target interventions and improve future activity.
- Assess human-related cyber security risks and determine, in consultation with relevant specialists and stakeholders, proportionate education, awareness, communications and behaviour-change interventions.
- Design and deliver engaging cyber security training and awareness materials for different audiences, translating technical security concepts, threats, policies and requirements into clear, accessible and actionable guidance.
- Build influential relationships with senior academic, professional and technical stakeholders across divisions, departments, faculties and colleges, using specialist expertise and evidence to secure engagement, influence local approaches and support adoption of University-wide cyber security requirements and good practice.
- Act as a specialist adviser on cyber security education, awareness and security behaviour, providing expert advice, recommendations and briefings to Cyber Security leadership, senior University stakeholders and relevant governance groups.
- Define the measures and evaluation framework for the education and awareness programme, using training, engagement, phishing, incident and behavioural data to assess effectiveness, identify emerging risks and determine priorities for future intervention.
- Analyse training, engagement, phishing and other relevant data to evaluate programme effectiveness, identify gaps and trends, and make evidence-based recommendations for improvement.
- Prepare reports, briefings and presentations on cyber security education and awareness activity, outcomes and risks for Cyber Security leadership and relevant governance groups.
- Develop and maintain cyber security communications channels and content, including relevant intranet content, guidance materials, campaigns and stakeholder/champion networks.
- Work with communications colleagues and Cyber Security subject matter experts to plan and coordinate communications supporting wider cyber security projects, services, policy changes and improvement initiatives.
- Contribute specialist expertise to the development and implementation of University cyber security policies, standards and guidance, assessing their implications for user behaviour and determining appropriate approaches to communication, education and adoption.
- Establish mechanisms for stakeholder and learner feedback and use the resulting evidence to continuously improve training, communications and engagement approaches.
- Identify opportunities to improve security culture and constructively challenge processes, communications or approaches where these create barriers to secure behaviour or effective risk reduction.
- Manage third-party suppliers and services supporting cyber security education, awareness, training and phishing simulation, defining requirements, monitoring service performance and value, resolving delivery issues and contributing to procurement, contract renewal and future service requirements.
- Maintain awareness of relevant cyber security threats, good practice, legislation, regulatory requirements and emerging approaches to security education and awareness, applying this knowledge to the University's activities.
- Work collaboratively with Cyber Security colleagues to ensure education and awareness activities respond appropriately to emerging threats, incidents, audit findings, assurance activity and organisational priorities.

- Represent the Cyber Security Education & Awareness function on relevant University working groups, networks and governance forums, providing specialist advice, influencing decisions and promoting a coordinated University-wide approach to security culture and behaviour.
- Line manage and develop staff within the Cyber Security Education & Awareness function, setting objectives and priorities, allocating work, managing performance and supporting professional development.

Selection criteria

Essential selection criteria

Education and Qualifications

- Educated to degree level or equivalent professional experience in cyber security, information technology, communications, organisational change, learning and development, education or a related discipline.

Experience

- Substantial experience of leading and developing education, awareness, communications, organisational change or behaviour-change programmes within a large and complex organisation.
- Demonstrable experience of developing strategy or strategic plans and translating organisational priorities, risks and evidence into programmes of activity.
- Experience of designing and delivering training, awareness campaigns or communications for large and diverse audiences.
- Experience of translating complex or technical information into clear, accessible and engaging material for non-specialist audiences.
- Experience of building effective working relationships with stakeholders across different professional disciplines and organisational levels.
- Experience of using data, management information and feedback to evaluate the effectiveness of training, communications or engagement activities and recommend improvements.
- Experience of leading complex programmes, projects or workstreams involving multiple stakeholder groups, competing priorities and significant organisational dependencies.
- Experience of working with external suppliers or service providers and monitoring delivery against agreed requirements.
- Experience of line management, supervising, coaching, mentoring or developing colleagues.

Knowledge and Capabilities

- Comprehensive knowledge of cyber security principles, common and emerging cyber threats, human-related cyber risk and the role of education, awareness and behaviour change in managing organisational security risk.
- In-depth understanding of cyber security education, awareness, security culture and behavioural-change approaches, with the ability to apply specialist knowledge to different risk profiles, audiences and organisational contexts.
- Excellent written, verbal and presentation skills, with the ability to communicate cyber security concepts effectively to both technical and non-technical audiences.
- Strong stakeholder engagement and influencing skills, with the ability to establish credibility and encourage adoption of good security practice without relying on formal authority.
- Strong analytical skills, with the ability to interpret information from multiple sources, identify trends and gaps, draw conclusions and make evidence-based recommendations.
- Ability to design and deliver engaging training, presentations, campaigns and supporting materials.
- Strong programme and project management skills, with the ability to establish priorities, manage interdependencies and resources, exercise independent judgement and deliver complex programmes of work against organisational objectives.
- Sound judgement and problem-solving skills, including the ability to identify issues, develop practical solutions and escalate significant risks appropriately.

- Understanding of relevant information security, data protection and regulatory requirements and their implications for staff awareness and behaviour.
- Ability to work independently while collaborating effectively as part of a multidisciplinary Cyber Security team.
- Trustworthy and able to handle sensitive security-related information appropriately.

Desirable selection criteria

- Relevant professional certifications such as CISMP, CompTIA Security+, ISO 27001 Foundation or similar. Project management, governance or risk-related qualifications would also be advantageous.
- Experience of working within the Higher Education sector, and/or an appreciation of the complexity of working across a highly federated organisation.
- Experience of delivering cyber security education and awareness programmes in a large, complex or federated organisation.
- Experience of phishing simulation, security behaviour measurement or cyber security training platforms (e.g., MetaCompliance).
- Experience of developing stakeholder or security champion networks.

Pre-employment screening

Standard checks

If you are offered the post, the offer will be subject to standard pre-employment checks. You will be asked to provide: proof of your right-to-work in the UK; proof of your identity; and (if we haven't done so already) we will contact the referees you have nominated. If you have previously worked for the University we will also verify key information such as your dates of employment and reason for leaving your previous role with the department/unit where you worked. You will also be asked to complete a health declaration so that you can tell us about any health conditions or disabilities for which you may need us to make appropriate adjustments.

Please read the candidate notes on the University's pre-employment screening procedures at:

<https://www.jobs.ox.ac.uk/pre-employment-checks>

About the University of Oxford

Welcome to the University of Oxford. We aim to lead the world in research and education for the benefit of society both in the UK and globally. Oxford's researchers engage with academic, commercial and cultural partners across the world to stimulate high-quality research and enable innovation through a broad range of social, policy and economic impacts.

We believe our strengths lie both in empowering individuals and teams to address fundamental questions of global significance, while providing all our staff with a welcoming and inclusive workplace that enables everyone to develop and do their best work. Recognising that diversity is our strength, vital for innovation and creativity, we aspire to build a truly diverse community which values and respects every individual's unique contribution.

While we have long traditions of scholarship, we are also forward-looking, creative and cutting-edge. Oxford is one of Europe's most entrepreneurial universities and we rank first in the UK for university spin-outs, and in recent years we have spun out 15-20 new companies every year. We are also recognised as leaders in support for social enterprise.

Join us and you will find a unique, democratic and international community, a great range of staff benefits and access to a vibrant array of cultural activities in the beautiful city of Oxford.

For more information, please visit www.ox.ac.uk/about/organisation.

University Administration and Services (UAS)

University Administration and Services (UAS) is the collective term for the professional services departments of the University, including IT Services and the Digital Governance Unit (the DGU). UAS comprises structures to:

- Support the University's core academic purposes of teaching, learning and research;
- Ensure the University can meet the requirements of government, funding bodies and other external agencies; and
- Facilitate the attainment of the objectives set out in the University's Strategic Plan.

The offices of the UAS sections are spread across the city centre, with the main University Offices located in Wellington Square.

For more information please visit: <http://www.admin.ox.ac.uk>

How to apply

Applications are made through our online recruitment portal. Information about how to apply is available on our Jobs website <https://www.jobs.ox.ac.uk/how-to-apply>.

Your application will be judged solely on the basis of how you demonstrate that you meet the selection criteria stated in the job description.

As part of your application you will be asked to provide details of two referees and indicate whether we can contact them now.

You will be asked to upload a CV and a supporting statement. The supporting statement must explain how you meet each of the selection criteria for the post using examples of your skills and experience. This may include experience gained in employment, education, or during career breaks (such as time out to care for dependants)

Please upload all documents **as PDF files** with your name and the document type in the filename.

All applications must be received by **midday** UK time on the closing date stated in the online advertisement.

Information for internal candidates

If you currently work at the University please note that:

- as part of the referencing process, we will contact your current department to confirm basic employment details including reason for leaving and information about your performance.
 - although employees may hold multiple part-time posts, they may not hold more than the equivalent of a full time post. If you are offered this post, and accepting it would take you over the equivalent of full-time hours, you will be expected to resign from, or reduce hours in, your other posts(s) before starting work in the new post.
 - Before applying for this post, you are advised to read the [Internal Mobility Principles](#). The principles promote good practice for moving into professional services roles, and are designed to provide clarity on expectations for managers and individuals.
-

Information for priority candidates

A priority candidate is a University employee who is seeking redeployment because they have been advised that they are at risk of redundancy, or on grounds of ill-health/disability. Priority candidates are issued with a redeployment letter by their employing department(s).

If you are a priority candidate, please ensure that you attach your redeployment letter to your application (or email it to the contact address on the advert if the application form used for the vacancy does not allow attachments).

If you need help

Application FAQs, including technical troubleshooting advice is available at:

<https://staff.web.ox.ac.uk/recruitment-support-faqs>

Non-technical questions about this job should be addressed to the recruiting department directly at

hr@ocdio.ox.ac.uk.

To return to the online application at any stage, please go to: www.recruit.ox.ac.uk.

Please note that you will receive an automated email from our online recruitment portal to confirm receipt of your application. **Please check your spam/junk mail** if you do not receive this email.

Important information for candidates

Data Privacy

Please note that any personal data submitted to the University as part of the job application process will be processed in accordance with the GDPR and related UK data protection legislation. For further information, please see the University's Privacy Notice for Job Applicants at: <https://compliance.admin.ox.ac.uk/job-applicant-privacy-policy>. The University's Policy on Data Protection is available at: <https://compliance.admin.ox.ac.uk/data-protection-policy>.

The University's policy on retirement

The University operates an Employer Justified Retirement Age (EJRA) for very senior research posts at **grade RSIV/D35 and clinical equivalents E62 and E82** of 30 September before the 70th birthday. The justification for this is explained at: <https://hr.admin.ox.ac.uk/the-ejra>.

For **existing** employees on these grades, any employment beyond the retirement age is subject to approval through the procedures: <https://hr.admin.ox.ac.uk/the-ejra>.

There is no normal or fixed age at which staff in posts at other grades have to retire. Staff at these grades may elect to retire in accordance with the rules of the applicable pension scheme, as may be amended from time to time.

Equal Opportunity

The University of Oxford is committed to equal opportunity, and to being a place where everyone belongs and is supported to succeed. We recognise how the diversity of our community enriches our ability to deliver on our academic mission.

We welcome applications from individuals from all backgrounds, including those under-represented within higher education. No applicant or members of staff shall be unlawfully discriminated against on the basis of age, disability, gender reassignment, marriage or civil partnership, pregnancy or maternity, race, religion or belief, sex, or sexual orientation.

Employment with the University and progression within employment will be determined according to personal merit and the application of criteria related to the duties and conditions of the post. In all cases, the primary consideration will be the ability to perform the job.

As stated in the University's Equality Policy and Equality, Diversity and Inclusion Strategic Plan, our commitment to equality and diversity goes hand in hand with our commitment to academic freedom and free speech.

Benefits of working at the University

Employee benefits

University employees enjoy 38 days' paid holiday, generous pension schemes, flexible working options, support for [sustainable travel](#) and other discounts. Staff can also access a huge range of personal and professional development opportunities. See <https://hr.admin.ox.ac.uk/staff-benefits>. Staff can access a huge range of personal and professional development opportunities. See <https://hr.admin.ox.ac.uk/staff-benefits>

Employee Assistance Programme

As part of our wellbeing offering staff get free access to a confidential employee assistance programme, available 24/7 for 365 days a year. Find out more at <https://staff.admin.ox.ac.uk/thriving-at-oxford>

University Club and sports facilities

Membership of the University Club is free for University staff. It offers social, sporting, and hospitality facilities. Staff can also use the University Sports Centre on Iffley Road at discounted rates, including a fitness centre, powerlifting room, and swimming pool. See www.club.ox.ac.uk and <https://www.sport.ox.ac.uk/>.

Information for staff new to Oxford

Please see our Life in Oxford webpage for information on relocating to and settling into the Oxford area. The website offers valuable guidance, including information on where to find more details about housing, transportation, finances, healthcare, and other key aspects of living in Oxford and the surrounding region. See [Life in Oxford | Oxford University Jobs](#)

There is also a visa loan scheme to cover the costs of UK visa applications for staff and their dependants. See <https://staffimmigration.admin.ox.ac.uk/visa-loan-scheme>

Family-friendly benefits

We are a family-friendly employer with one of the most generous family leave schemes in the Higher Education sector (see <https://hr.web.ox.ac.uk/family-leave>). Our Childcare Services team provides guidance and support on childcare provision, and offers a range of high-quality childcare options at affordable prices for staff. In addition to 5 University nurseries, we partner with a number of local providers to offer in excess of 450 full time nursery places to our staff. Eligible parents are able to pay for childcare through salary sacrifice, further reducing costs. See <https://childcare.admin.ox.ac.uk/>.

Supporting disability and health-related issues (inc menopause)

We are committed to supporting members of staff with disabilities or long-term health conditions, including those experiencing negative effects of menopause. Information about the University's Staff Disability Advisor, is at <https://edu.admin.ox.ac.uk/disability-support>. For information about how we support those going through menopause see <https://hr.admin.ox.ac.uk/menopause-guidance>

Staff networks

The University has a number of staff networks including for research staff, BME staff, LGBT+ staff, disabled staff network and those going through menopause. Find out more at <https://edu.admin.ox.ac.uk/networks>

The University of Oxford Newcomers' Club

The University of Oxford Newcomers' Club is run by volunteers that aims to assist the partners of new staff settle into Oxford, and provides them with an opportunity to meet people and make connections in the local area. See www.newcomers.ox.ac.uk.

Research staff

The Researcher Hub supports all researchers on fixed-term contracts. They aim to help you settle in comfortably, make connections, grow as a person, extend your research expertise and approach your next career step with confidence. Find out more <https://www.ox.ac.uk/research/support-researchers/researcher-hub>

Oxford's Research Staff Society is a collective voice for our researchers. They also organise social and professional networking activities for researchers. Find out more <https://www.ox.ac.uk/research/support-researchers/connecting-other-researchers/oxford-research-staff-society>