

Job title Identity Manager

Department:	IT & Digital Services (ITDS).
Grade / Salary:	Grade 9 / (£63,655 - £71,157)
Contract Type:	Permanent
Hours:	35 Hrs per week (Full time)
Location:	Hybrid – New Cross Campus / Remote

Goldsmiths

Goldsmiths, University of London is a world-leading centre of educational excellence where ground-breaking research meets innovative teaching and thinking. We're looking for inspiring and talented people to help build on our global reputation while also growing personally in a true learning organisation.

As a college we are working to tackle inequality in all its forms and are working to promote equality on grounds of race, disability, age, sex, gender identity, sexual orientation, religion and belief, marriage and civil partnership, pregnancy and maternity, and caring responsibilities. We are keen to attract candidates from diverse backgrounds who share our commitment to creating an inclusive culture in which all students and staff can thrive.

Information for candidates with disabilities can be found on our [Disability & Individual needs](#) page. We are happy to supply information in alternative formats for disabled applicants. Please contact hr-recruitment@gold.ac.uk to make your request.



Department of ITDS

The Department of IT & Digital Services (ITDS) is responsible for providing IT and Digital services to support the learning, teaching, research, and administrative work of Goldsmiths. The Department plays a key role in ensuring that staff and students have excellent digital experiences that enhance their experience of working and studying at the College. The Department also plays a vital role in developing and supporting all major business systems, ensuring that products and services are resilient and can meet user needs.

Our digital principles underline all our work:

- We put people at the heart of everything we do
- We are bold and open to change
- We create digital first, responsive and accessible services
- We use data and insight to drive our decisions
- We measure, test and learn
- We engage, collaborate and partner
- We provide a safe and secure service
- Our systems are flexible, sustainable and interoperable

Job description

Reporting to: Head of IT Delivery and Governance

Reports: None

Summary:

The **Identity Manager** will play a critical role within the IT & Digital Services (ITDS) department, responsible for developing, implementing, and managing the Universities' identity and access management (IAM) strategy. This role ensures secure, efficient, and seamless access to systems and services for staff, students, and partners while maintaining compliance with regulatory requirements.

You will be the subject matter expert on IAM, working across the institution to safeguard user identities, manage authentication and authorisation processes, and ensure integration between enterprise systems, cloud platforms, and security frameworks.

Main duties:

- Lead the design, implementation, and ongoing management of the institution's identity and access management strategy.
- Manage identity lifecycle processes, including onboarding, provisioning, de-provisioning, and access reviews.
- Implement and maintain solutions for Single Sign-On (SSO), Multi-Factor Authentication (MFA), and privileged access management.
- Ensure compliance with relevant regulations and security standards such as GDPR, ISO27001, PCI DSS, and Cyber Essentials.
- Responding to requests from the ICO, and FOI requests.
- Act as the primary point of contact for all IAM-related projects and BAU activities, liaising with internal stakeholders, security teams, and third-party vendors.
- Oversee integration of IAM solutions with cloud platforms, enterprise applications, and core business systems.
- Develop and maintain IAM policies, procedures, standards and proactive monitoring mechanisms
- Report on IAM operations, including security incidents, access violations, and audit findings.
- Own and oversee the full IAM technology stack, ensuring systems are well-maintained, upgraded, and aligned with institutional needs
- Collaborate closely with the cybersecurity and infrastructure teams to ensure identity-related risks are identified, mitigated, and documented.
- Provide expertise and leadership on authentication protocols (e.g. SAML, OAuth, OpenID Connect, LDAP).
- Lead user education and awareness initiatives to promote secure identity and access practices.

Person Specification

Detailed below are the types of qualifications, experience, skills, and knowledge which are required of the post holder. Selection will be made upon evidence of best fit with these criteria.

Experience

- Proven experience in identity and access management within a complex organisation.
- Experience implementing and managing IAM platforms (e.g., One Identity Manager, Okta, Azure AD, Entra ID, Ping Identity, ForgeRock).

- Demonstrated expertise with authentication and authorisation protocols.
- Experience integrating on-premises and cloud-based identity systems.
- Hands-on experience with privileged access management and role-based access control (RBAC).
- Knowledge of cybersecurity principles and their application within IAM.
- Experience conducting access audits and ensuring regulatory compliance.

Skills, Abilities & Knowledge

- In-depth understanding of One Identity product suite
- In-depth understanding of identity governance, authentication protocols, and access provisioning workflows.
- Familiarity with IAM tools, security frameworks, and enterprise directory services (e.g., Active Directory, LDAP, Entra ID, Okta).
- Knowledge of compliance and data protection standards, including GDPR, ISO27001, WCAG 2.1, SOC1, SOC2 and Cyber Essentials.
- Audit compliance, audit governance and audit readiness experience.
- Excellent analytical, problem-solving, and decision-making skills.
- Strong stakeholder engagement and the ability to explain technical concepts to non-technical audiences.
- Capability to manage IAM-related risks and implement remediation strategies.
- Strong Microsoft Windows Server and Azure skills. Linux a bonus.
- PowerShell and/or other scripting language skills.

Values & Personal Qualities

- Strong commitment to security, data privacy, and regulatory compliance.
- Collaborative, user-focused approach to technology delivery.
- Ability to thrive in a fast-paced, dynamic environment.
- Proactive, adaptable, and highly organised.

Education & Qualifications

- Professional certifications such as CISSP, CISM, Microsoft Certified: Identity and Access Administrator, Okta Certified Professional, or equivalent is highly desirable.
- ITIL, PRINCE2, or Agile qualifications are advantageous.

The Essential criteria sections show the minimum essential requirements for the post, therefore if you cannot demonstrate in your application that you meet the essential criteria categorised below, you will not be invited to interview.

The Desirable criteria sections show additional attributes which would enable the applicant to perform the role more effectively with little or no training.

The Category column indicates the method of assessment:

A = Application form

I = Interview

T = Test

C = Certificate

R = Reference

P = Presentation

	Category
Essential Criteria 1 - Qualifications	
Microsoft Certified: Identity and Access Admin	C
Desirable Criteria 1 - Qualifications	
Certifications such as ITIL, PRINCE2 or Agile practitioner	C
Essential Criteria 2 - Experience	
Proven experience in a similar role with 5+ years of experience	A & I
Desirable Criteria 2 - Experience	
Experience in working in, or with, a service delivery organisation and the ITIL framework	A & I
Audit compliance, audit governance and audit readiness experience	A & I
Essential Criteria 3 – Knowledge	
In depth understanding of identity and access management concepts, role-based access control, authentication protocols, SSO components and solutions including Entra ID, Okta, One Identity Manager	A & I
Familiarity with GDPR, SOC1, SOC2, ISO27001	A & I
Knowledge of Active Directory, Azure AD, Windows Server	A & I
Desirable Criteria 3 - Knowledge	
Knowledge of higher education specific identity challenges	A & I
PowerShell (or similar) scripting skills	A & I
Essential Criteria 4 - Skills	
Excellent analytical, problem-solving, and decision-making skills	A & I

Strong communication and interpersonal skills, with the ability to work effectively with diverse teams and stakeholders	A & I
Confident in influencing, engaging, and negotiating with multiple stakeholders, and able to challenge constructively and receive challenges	A & I
Ability to lead cross-functional teams, manage stakeholders and drive consensus	A & I
Desirable Criteria 4 - Skills	
Proven ability to lead or contribute to IAM-related user education, training programs, and awareness campaigns.	A & I

Please also note that where qualifications are required, employment is conditional on the verification of them. Qualifications (must be original documents) will be checked on or before the first day of appointment.

Summary of Benefits

If you choose to work with us, you'll become part of a learning organisation that is committed to professional and personal development, with comprehensive and innovative staff development and wellbeing programmes.

You'll also have access to frequent lunchtime and evening talks, seminars and performances, and annual performance and development reviews.

Our other benefits include:

- Competitive salary
- Working in Zone 2, with fantastic transport links and interest free travel to work loans
- Excellent annual leave entitlement plus additional closure days at Christmas and Easter
- 3 days of volunteering leave per annum, plus parental and study leave allowance.
- Maternity, paternity, shared parental leave and adoption leave and pay
- Membership of USS or LPFA pension scheme, dependent upon grade
- Contractual sick pay provision
- Access to an Employee Assistance Programme, offering 24/7/365 confidential and free advice, support, and information service on a range of personal, family, or work-related matters.

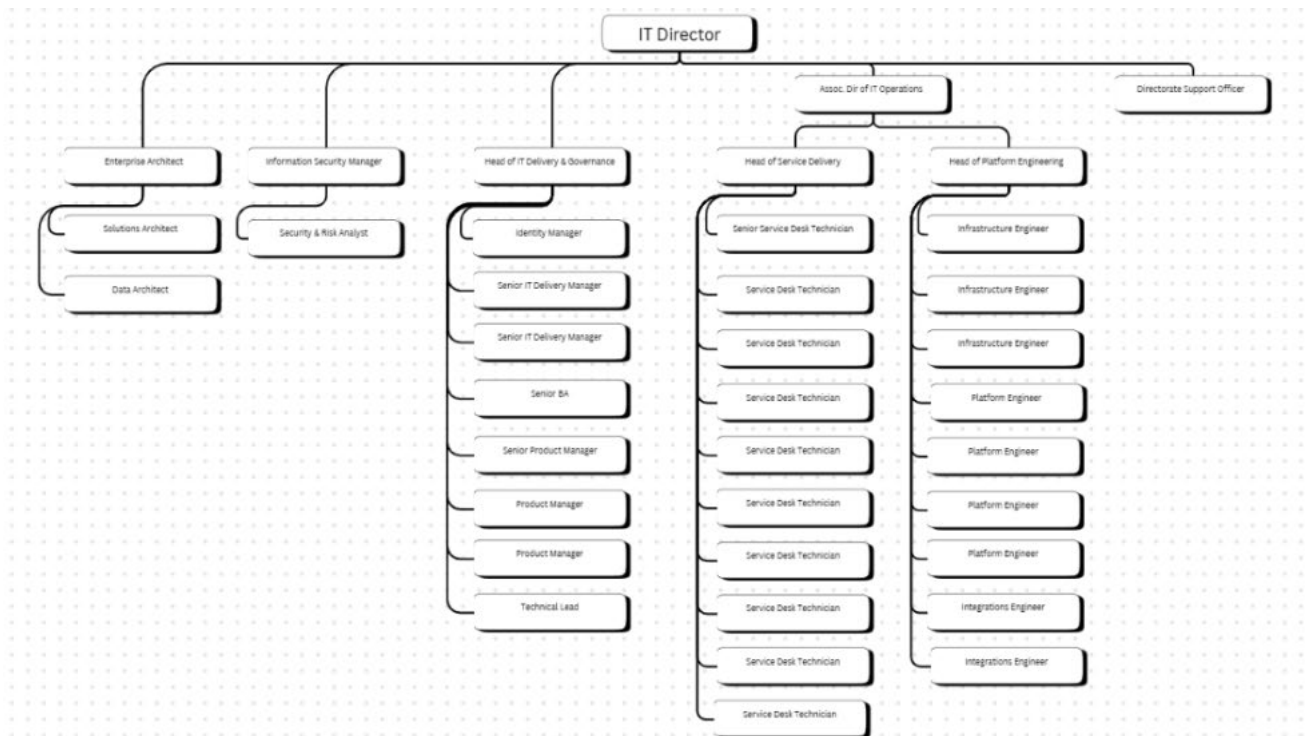
- Free eye tests
- Cycle to work scheme
- Wellbeing initiatives including the Chaplaincy and Staff Choir
- On-site dining facilities
- Access to University of London facilities such as Senate House Library
- Membership of Staff Diversity Networks: (Dis)Ability, Goldsmiths Race Equality Group, LGBTQ+, Menopause, Parents and Carers, Women at Goldsmiths. (Staff are also encouraged to join networks as Allies should they wish to do so rather than as members)

Further information

For more information about Goldsmiths, please visit: www.gold.ac.uk/about

Thank you for your interest in working with us, we wish you all the best with your application.

Appendix 1.



Future Org (38 roles)