

# UCL Information Risk Governance Committee Terms of Reference

## Purpose

The UCL Information Risk Governance Committee (IRGC) is a senior-level governance board that is a sub-committee of the Digital Strategy Committee. The primary responsibility for the IRGC is to oversee and approve the implementation of UCL's information governance policy and strategies to protect its information assets in line with UCL's risk appetite. It ensures the alignment of these policy and strategies with UCL's objectives.

## Scope and context

The IRGC's scope includes the security of all UCL information assets. This includes cyber security compliance and data protection.

- The CISO owns UCL's Information Security policy and Strategy
- The Data Protection Officer owns the Data Protection policy and Strategy
- The IRGC provides oversight of both policies and strategies
- The IRGC reports, via the SIRO, to the Digital Strategy Committee

## Objectives

These objectives are owned by the Senior Information Risk Owner (SIRO). The SIRO chairs the IRGC

## Strategic

- Establish accountability, responsibility and authority. The IRGC sets the roles, responsibilities and the authorities for the protection of the organization's information assets.
- Ensure, via the Digital Strategy committee, activities to manage information risk are adequately resourced.
- Inform UCL's risk appetite in the context of information risks from across the organisation.
- Approve the Information Security and Data Protection policies and strategies, thus ensuring that UCL's objectives are properly supported.

## Risk oversight

- Act as a point of escalation for issues relating to security and information risk management.
- Decide on escalated exceptions which require UCL's risk appetite to be exceeded.
- Track progress of actions related to escalated exceptions and other relevant information security risks.
- Approve changes to information security and data protection policies.
- Handle escalations arising from policy exemption requests; Decisions of the IRGC may be formalized as new or updated policies.

## Monitoring

- Agree on metrics that indicate the effectiveness of UCL's information security and data protection strategies
- Agree annual targets for those metrics.
- Review performance against agreed targets.
- Provide recommendations for the security programme based on findings from incidents, audit and observations.
- Review incident trends affecting UCL information assets.

## Other

- Be the authority where there is duplication of information governance oversight with other groups / committees / within UCL
- Lead by example:
  - foster an environment where information security is considered second nature for all members of UCL
  - act as information security and data protection advocates
- Review these terms of reference at least annually, updating them as needed to respond to internal and external changes or requirements.
- The committee shall review its own performance annually.

## Meeting frequency

The committee will meet once per term. Extraordinary meetings may be called in response to issues arising from serious incidents.

Papers will be available a minimum of one week before the date of the meeting.  
Minutes will be made available to committee members after initial review by the chair.

Some papers will contain confidential information. These will be marked for clarity.

## Appendix A - membership and roles

The members of IRGC include

Name	Role
Professor Mark Emberton	Dean, Faculty of Medical Sciences Senior Information Risk Owner (SIRO) and chair
Sarah Lawson	Chief Information Security Officer (CISO)
Alex Potts	Data Protection Officer (DPO)
Trevor Peacock	Information Governance Lead
Natasha Lewis	General Counsel, Legal Services
Donna Dalrymple	Director, Human Resources / TOPS
Charu Gorasia	Head of Finance
Mark West	Security Manager, Estates
Sarah Cows	Director, Student and Registry Services, Registrar (interim)
SU Education Officer	Students' Union
Dean Stokes	Director, Planning
Professor Madeline Carr	Professor of Global Politics and Cyber Security, Computer Science
Professor Richard Gilson	Director, UCL Centre for Clinical Research in Infection and Sexual Health, Deputy SIRO
Rajinder Sidhu	Associate Director, Research Governance and Operations UCLH/UCL JRO
Dr James Hetherington	Director, The Centre for Advanced Research Computing (ARC)
Tim Machin	Head of Faculty IT, Population Health Sciences, Chair of the Operational Management Group (OMG)
Alison Amatsah	Data Governance Manager, OVP (Strategy)
Dr Paul Lamb	Chair, Security Working Group and Head of Computing, MSSL

### Quorum

Half of the membership with:

SIRO or Deputy SIRO

Plus

CISO or deputy CISO

Plus

DPO or deputy DPO

The membership will be reviewed annually

Members will be asked annually to declare any conflicts of interest

## Appendix B – standing agenda

1. Approval of last meeting's minutes
2. Matters arising
3. Threats to UCL
  - 3.1. Cyber threats - *overview of emerging and current threats to UCL*
4. Risk scoring -
  - 4.1.1. Metrics and trends
5. Reporting – updates, activities and factors affecting information risk  
*Internal and external factors that improve or impact UCL's information risk profile*
  - 5.1. Data protection
  - 5.2. Information Security Group
  - 5.3. Outreach
  - 5.4. Audits
  - 5.5. Compliance - *receive reports on the Data Safe Haven and other areas for which the Committee represents UCL's leadership*
6. Risk updates by sector – *feedback on factors affecting information risk*
  - 6.1. HR
  - 6.2. ISD
  - 6.3. Finance
  - 6.4. etc.
7. Items requiring committee decision / action / approval
  - 7.1. Papers
  - 7.2. Policy changes
  - 7.3. Escalations
8. Opportunities to link UCL research with UCL's information risk activities
  - 8.1. Updates
  - 8.2. New opportunities
9. AOB