CLIMB Acceptable Use Policy

Version 3.1
Date published: 01 November 2025
Valid from: 01 December 2025

1. Introduction and Scope

1.1 Purpose

This Acceptable Use Policy governs the use of CLIMB (Cloud Infrastructure for Microbial Bioinformatics), a specialised cloud computing platform designed for microbial bioinformatics research. CLIMB operates as a partnership between the Quadram Institute Bioscience (QIB) and the University of Birmingham, providing research computational resources and services to the UK and international microbial bioinformatics community. This policy applies to all users regardless of their institutional affiliation or user category.

1.2 Scope

This policy applies to all users of CLIMB services, including:

- Primary users (UK-based with institutional oversight responsibilities)
- Secondary users (including international collaborators under primary user responsibility)
- External researchers accessing CLIMB through research and service collaborations
- Industrial users under specific research and service collaboration agreements
- All persons accessing CLIMB resources through any access method regardless of their location or institutional affiliation

1.3 Compliance Framework

This policy should be read in conjunction with the CLIMB Terms and Conditions, which govern the contractual relationship, service provision, and operational aspects of CLIMB usage.

Users must comply with:

- This CLIMB Acceptable Use Policy
- CLIMB Terms and Conditions, which govern the contractual relationship, service provision, and operational aspects of CLIMB usage
- UK legislation including Data Protection Act 2018, GDPR, Computer Misuse Act 1990
- International laws applicable to their jurisdiction
- Specific terms of research collaboration agreements

2. Who Can Access CLIMB

2.1 Primary Users

Primary users must be UK-based and include:

- Staff with salaried positions in UK academic institutions (.ac.uk email)
- Staff in UK government agencies (.gov.uk email)
- Staff in UK healthcare systems (.nhs.uk email)
- Staff who have independent researcher status and/or team leadership responsibilities
- Industrial users under approved research collaboration agreements with CLIMB

Primary User responsibility

- Maintain eligibility throughout the access period
- Take full responsibility for all secondary users they sponsor
- Ensure compliance with UK institutional and legal requirements
- Serve as the primary point of contact for their team

2.2 Secondary Users

Secondary users work under the supervision and responsibility of a primary user and may include:

- PhD students and postdoctoral researchers (UK and international)
- Research technicians and bioinformaticians (UK and international)
- International collaborators and visiting researchers
- Industrial employees under collaboration agreements
- Researchers from international institutions engaged in collaborative projects with CLIMB

International Secondary User Framework:

- International secondary users must be sponsored by a UK-based primary user
- Primary user maintains full responsibility for international secondary user compliance
- Access is contingent on ongoing collaboration with the sponsoring primary user
- International users must comply with UK laws and institutional policies while using CLIMB

2.3 Research Collaboration Framework

External organisations may access CLIMB through formal research and service collaboration agreements, industry partnership programmes or approved training and capacity building initiatives.

International partnerships must comply with relevant data sovereignty and export control requirements.

3. Acceptable Uses

3.1 Primary Permitted Activities

CLIMB is provided primarily for:

- Microbial bioinformatics research and analysis
- Pathogen genomics and surveillance
- Public health genomics applications and emergency response activities
- Collaborative research projects between institutions
- Training and educational activities in bioinformatics
- Development and testing of bioinformatics tools and workflows

3.2 Research Collaboration Activities

Users may access CLIMB for:

- Multi-institutional research projects with clear academic objectives
- International research collaborations with appropriate oversight
- Industry-academic partnerships under approved agreements
- Capacity building and training initiatives
- Open science and reproducible research activities

3.3 Conditional Users

The following activities require prior approval from CLIMB management:

- Research activities outside the core microbial bioinformatics scope
- Large-scale computational projects that may impact other users
- Data sharing arrangements involving sensitive or restricted datasets
- Commercial research activities beyond established collaboration frameworks
- Activities involving export-controlled technologies or data

3.4 Academic Freedom

Nothing in this policy is intended to limit academic freedom. Research involving controversial or sensitive materials may be permitted with appropriate approval from institutional Research Governance, Ethics and Integrity Committees in consultation with CLIMB management, provided such research complies with legal requirements and institutional ethics frameworks.

4. Prohibited Uses

4.1 Strictly Prohibited Activities

Users must never:

- Use CLIMB for illegal activities or activities violating institutional policies, UK laws or relevant international laws
- Engage in hacking, unauthorized access, or security breaches
- Host, distribute, or create illicit or illegal media
- Conduct cryptocurrency mining or similar resource-intensive non-research activities
- Share access credentials with unauthorized individuals
- Attempt to compromise system security or stability
- Use the platform for purely commercial purposes without appropriate agreements

Users must not create, store, or transmit materials that may constitute or incite criminal activity related to terrorism, including encouraging terrorism, inviting support for proscribed terrorist organisations, or materials prohibited by the Terrorism Act 2006 or Counter-Terrorism and Security Act 2015.

4.2 Research Integrity Violations

Users must not:

- Engage in research misconduct including data fabrication or falsification
- Violate research ethics approvals or institutional review board requirements
- Infringe intellectual property rights, copyright, or licensing terms
- Misrepresent research findings, data ownership, or institutional affiliations
- Violate data sharing agreements or confidentiality requirements
- Fail to provide appropriate acknowledgement of CLIMB in publications

Users must not introduce any software or materials requiring a licence for which a valid licence is not in place. Users must take reasonable care to prevent illicit copying of licensed software and documentation.

4.3 Harmful or Offensive Content

Users must not create, store, or transmit:

- Content that violates laws regarding harassment, discrimination, or hate speech
- Defamatory, threatening, or offensive materials
- Malicious software, viruses, or security threats
- Unauthorised personal data or confidential information
- Materials that could harm CLIMB's reputation or that of partner institutions

When using CLIMB systems for communications or social media that reference CLIMB, users must: make clear they speak on their own behalf unless specifically authorised by CLIMB management; not damage CLIMB's reputation or that of partner institutions; not harass, bully, or discriminate against others; and not breach confidentiality, data protection, or intellectual property requirements.

Users must not use CLIMB systems to impersonate another individual, organisation, or entity, whether real or fictitious.

4.4 Clinical Data Restrictions

- Storing patient identifiable data is strictly prohibited
- Users must ensure appropriate de-identification of any health-related data

- Clinical research data must be de-identified and must comply with relevant ethics approvals and data protection regulations

5. User Responsibilities

5.1 Security Responsibilities

All users must:

- Use strong, unique passwords and enable two-factor authentication
- Report security incidents or suspected breaches immediately
- Keep access credentials confidential and secure
- Log out of systems when not in active use

5.2 Data Management Responsibilities

Users are responsible for:

- Classifying data appropriately and applying suitable protection measures
- Implementing adequate backup strategies for critical data
- Complying with data protection legislation (GDPR, national laws)
- Respecting data retention policies and license periods
- Obtaining necessary permissions for data sharing and collaboration

5.3 Resource Usage Responsibilities

Users must:

- Use computational resources efficiently and responsibly
- Avoid wasteful or excessive resource consumption that affects other users
- Follow guidance on appropriate resource allocation for different workloads
- Properly manage and clean up unused resources (notebooks, storage)
- Respect priority access arrangements for emergency response activities

5.4 Collaborative Responsibilities

Primary users must:

- Take responsibility for all secondary users they sponsor (including international users)
- Ensure secondary users understand and comply with this policy
- Maintain oversight of international users' activities
- Remove access for secondary users who leave their teams or complete collaborations
- Keep contact information current for themselves and their team members
- Ensure compliance with UK institutional and legal requirements
- Inform CLIMB management of significant changes in eligibility or status

Users allocated CLIMB identifiers (userIDs, passwords, credentials) must make all reasonable efforts to maintain their confidentiality and integrity. Users must report any suspected breach of security immediately. Use of resources allocated to another user is prohibited unless specifically authorised by CLIMB management.

5.5 Acknowledgement Requirements

All users must acknowledge CLIMB in all publications, presentations and reports using CLIMB resources and notify CLIMB of publications arising from CLIMB-supported research.

6. International Collaboration Guidelines

All international access must be through UK-based primary users, who maintain legal and operational responsibility for international secondary users.

International users must comply with UK data protection requirements and cross-border data transfers must comply with relevant legal frameworks.

7. Monitoring and Compliance

7.1 Usage Monitoring

CLIMB administrators may monitor:

- System performance and resource utilisation patterns
- Compliance with usage policies and security requirements
- Network traffic for security threats and policy violations
- Data transfer activities for unusual or suspicious patterns

7.2 Investigation Authority

CLIMB reserves the right to:

- Investigate suspected policy violations or security incidents
- Access user data and communications for legitimate operational or security purposes
- Cooperate with institutional authorities and law enforcement as required by law
- Suspend access pending investigation of serious violations

Using CLIMB systems to commit violations against external systems (outside CLIMB) also constitutes a policy violation and may result in enforcement action.

8. Consequences of Policy Violations

8.1 Progressive Enforcement

Policy violations may result in:

- Warning: Documentation of violation with guidance for compliance

- Temporary Suspension: Short-term access restriction with conditions for restoration
- Package Termination: Removal of access package
- Account Termination: Permanent removal of access privileges
- Institutional Referral: Reporting to user's home institution for disciplinary action
- Legal Action: Referral to law enforcement for criminal activities

8.2 Factors Considered in Enforcement

- Severity and impact of the violation
- Intent (accidental vs. deliberate)
- User's response and cooperation
- History of previous violations
- Risk to system security or other users

8.3 Appeal Process

Users may appeal enforcement actions through:

- Initial review by CLIMB management team
- Escalation to institutional authorities where appropriate
- Independent review for serious sanctions

9. Policy Governance

9.1 Policy Authority

This policy is maintained by CLIMB management in consultation with:

- Partner institution information security teams
- Research governance and ethics committees
- User community representatives
- Legal and compliance advisors

9.2 Updates and Communication

- Policy updates will be communicated through official CLIMB channels
- Users will be notified of significant changes affecting their access or obligations
- Regular review ensures the policy remains current and effective

9.3 Questions and Clarifications

For questions about this policy, contact climb@quadram.ac.uk