BJRI DIGITAL SAFEGUARDING CYBER SECURITY AND RESPONSIBLE ONLINE INSTITUTIONAL CONDUCT FRAMEWORK

BLACK JUSTICE RESEARCH INSTITUTE

Digital Safeguarding and Cyber Security Governance Framework

---

1. PURPOSE

The purpose of this framework is to establish the digital safeguarding, cyber-security, lawful conduct, evidential discipline, and responsible online institutional behaviour principles governing the digital activities of the Black Justice Research Institute (“BJRI”).

The Institute recognises that digital conduct and cyber-security responsibilities are necessary to support safeguarding, public confidence, institutional credibility, procedural fairness, and responsible information management.

2. CORE DIGITAL GOVERNANCE PRINCIPLES

The Institute supports:

- lawful digital conduct,
- safeguarding awareness,
- cyber-security responsibility,
- evidential discipline,
- proportionality,
- analytical restraint,
- and responsible communication standards.

The Institute rejects:

- harassment,
- intimidation,
- coercive digital practices,
- inflammatory escalation behaviour,
- reckless publication activity,
- and manipulative online conduct.

3. DIGITAL SAFEGUARDING RESPONSIBILITIES

The Institute recognises safeguarding obligations within:

- online publication activity,
- digital communications,
- research dissemination,
- archive management,
- institutional websites,
- and social media activity.

Digital activity should therefore support public protection, lawful conduct, safeguarding awareness, and reduction of unnecessary escalation risks.

4. CYBER-SECURITY PRINCIPLES

The Institute recognises:

- cyber-security risks,
- unauthorised access risks,
- reputational safeguarding concerns,
- data integrity risks,
- and digital escalation risks.

Institutional digital systems should therefore support:

- responsible access control,
- careful data management,
- safeguarding awareness,
- lawful conduct,
- and evidential preservation where appropriate.

5. EVIDENTIAL DISCIPLINE

The Institute distinguishes between:

- verified fact,
- allegation,
- disputed claim,

• reported experience,
• hypothesis,
• perception,
• and speculation.

Digital publication activity should therefore avoid presenting allegation or speculation as verified fact without appropriate evidential foundation.

6. RESPONSIBLE ONLINE COMMUNICATION

Online communication associated with the Institute should support:

• procedural fairness,
• analytical restraint,
• responsible communication standards,
• safeguarding awareness,
• and lawful conduct.

The Institute rejects:

• inflammatory rhetoric,
• harassment campaigns,
• coercive online behaviour,
• manipulative communication practices,
• and reckless digital escalation.

7. DIGITAL ARCHIVE AND INFORMATION RESPONSIBILITIES

The Institute supports responsible digital preservation of:

• governance frameworks,
• safeguarding documentation,
• research publications,
• institutional records,
• and public-interest materials.

Digital archive management should support evidential integrity, institutional continuity, and responsible public access where reasonably appropriate.

8. PUBLIC TRUST AND RESPONSIBLE DIGITAL CONDUCT

The Institute recognises that institutional credibility depends substantially upon:

- responsible digital conduct,
- safeguarding seriousness,
- lawful communication standards,
- evidential discipline,
- proportionality,
- and cyber-security awareness.

9. CONCLUSION

The Institute’s digital safeguarding and cyber-security framework is grounded in evidential discipline, safeguarding awareness, lawful conduct, procedural fairness, analytical restraint, and responsible online institutional behaviour.

The Institute supports calm, evidence-based, proportionate, and responsible digital engagement practices consistent with long-term institutional credibility.