Christ the Redeemer College London

IT AND CYBER SECURITY POLICY

The purpose of this policy is to provide guidance on the safe and responsible use of information technology (IT) including artificial intelligence (AI) applications and the application of technologies, processes, and controls to protect systems, networks, programs, devices and data at Christ The Redeemer College (CRC) from cyber-attacks.

Scope

This policy applies to all students, faculty, staff, and visitors who access, store, transmit or process CRC data or use CRC's IT systems or networks either offline (including on the local network) or online (over the wider internet). It covers all devices connected to the college network and any external networks used to access college resources.

This policy should be used in conjunction with CRC's IT Acceptable Usage Policy.

Acceptable Use

CRC is committed to protecting the confidentiality, integrity and availability of its data and IT resources from unauthorised access, misuse, modification, disruption, or destruction. All data sensitivity classifications and applied security controls must be complied with accordingly.

CRC also recognises the potential benefits and risks of using AI for various purposes, such as education, research, administration, and innovation.

Therefore, CRC expects all users of IT and online resources to adhere to the following principles:

1. Respect the rights and privacy of others.
    1.1. Users must not access, disclose, copy, modify or delete any data or IT systems and resources that they are not authorised to access or that belong to others without their consent.
    1.2. Users must also comply with all applicable laws and regulations regarding data protection and privacy, such as the General Data Protection Regulation (GDPR) and The Data Protection Act (2018).

2. Use IT, AI, and online resources for authorised purposes only.

2.1. Users must not use IT and online resources for illegal, unethical, fraudulent, malicious, or harmful activities, such as hacking, phishing, spamming, cyberbullying, harassment, discrimination, or plagiarism.
2.2. Users must also not use IT, AI, or online resources for personal gain or commercial purposes that are not related to CRC's mission and goals.

3. Protect IT, online, and cyber security resources from threats.
3.1. Users must take reasonable measures to safeguard their accounts, passwords, devices and data from unauthorised access or loss.
3.2. Users must also report any suspected or actual incidents of IT or cyber security breaches to CRC's IT department as soon as possible.
3.3. Users must not install or use any software or hardware that may compromise the security or performance of CRC's IT systems or networks, such as malware, viruses, spyware, or unauthorised wireless access points.

4. Use AI responsibly and ethically.
4.1. Users must ensure that any AI applications they develop, or use are aligned with CRC's values and principles, as well as with the ethical standards and best practices of their respective fields.
4.2. Users must also consider the potential impacts and implications of AI on society, human rights, diversity, inclusion, and sustainability.
4.3. Users must not use AI for purposes that may cause harm or injustice to individuals or groups, such as discrimination, bias, manipulation, or deception.

5. Mitigate risks of generative AI usage.
5.1. Users must not enter or upload personal information into generative AI systems. This includes names, dates of birth, addresses, pictures of people and other private data (such as identity documents). Where there is legitimate need to upload personal or private documents (such as getting recommendations on improving content, users must first redact all personal details).
5.2. Users must not enter or upload confidential work or college information into generative AI systems. This includes bank statements, and other internal organisational information.
5.3. Users must not enter, or upload copyrighted or copy-protected materials into generative AI systems.
5.4. CRC will inform and educate users about acceptable generative AI usage in line with academic integrity policies and expectations. These provide clear guidelines on what is, and what is not acceptable.
5.5. CRC will promote critical thinking skills on how to evaluate information generated by AI systems.
5.6. CRC will promote digital and AI literacy, and support users in gaining a deeper understanding of generative AI and its usage.

6. Acknowledge sources and contributions.
   6.1. Users must give proper credit and attribution to the original sources and contributors of any data, software, code, algorithms, or models that they use or reuse for AI or other applications.
   6.2. Users must also respect the intellectual property rights and licenses of others when using their IT and cyber security resources.

Safeguards and Controls

CRC's security implementations include:

1. Data Security and Privacy:
   1.1. Data encryption during transmission and storage.
   1.2. Regular data backup and off-site (cloud) storage.
   1.3. Access controls based on the principle of least privilege.
   1.4. Compliance with data protection laws and regulations.
   1.5. Secure disposal of data in accordance with college policies.
   1.6. Periodic data audits and risk assessments.

2. Network Security:
   2.1. CRC maintains a secure network infrastructure to protect against unauthorised access, data breaches, and other network-related threats.
   2.2. CRC's network security procedures include:
      2.2.1. Use of firewalls, intrusion detection/prevention systems, and network segmentation.
      2.2.2. Regular monitoring of network traffic and security logs.
      2.2.3. Secure configuration of network devices and equipment.
      2.2.4. Authentication mechanisms, such as strong passwords, multi-factor authentication, and secure Wi-Fi protocols.
      2.2.5. Regular security assessments and vulnerability scanning.

3. System Security:
   3.1. CRC implements measures to secure computer systems, servers, and software.
   3.2. CRC's procedures for system security include:
      3.2.1. Regular patching and updates of operating systems and applications.
      3.2.2. Use of reputable antivirus and anti-malware software.
      3.2.3. Implementation of secure configurations and access controls.
      3.2.4. Monitoring and logging of system activities.
      3.2.5. Application of incident response and recovery plans for system breaches or failures.

4. Incident Response:
   4.1. CRC maintains an incident response plan to detect, respond to, and recover from security incidents in a timely and effective manner.

4.2. Users should report any suspected or observed security incidents to the IT department.

4.3. The following outlines CRC's response in the event of a cyberattack, data breach, or other IT-related emergency (scope of coverage can be found in the college's Business Continuity Plan document):

4.3.1. Roles and responsibilities: The CRC IT Manager oversees the incident response team. This individual will communicate with stakeholders, while technical tasks and support will be provided by all members of the IT team.

4.3.2. Incident classification: Incidents are categorised based on their severity, impact, and urgency. Low-level incidents include minor system glitches, while high-level incidents include ransomware attacks.

4.3.3. Incident notification: Depending on incident classification, relevant parties, such as management, customers, vendors, law enforcement, and regulators may need to be notified.

4.3.4. Incident containment: Isolation and prevention of the spread of the incident will be carried out through methods such as disconnecting affected devices, cutting internet access, blocking malicious traffic, or restoring backups.

4.3.5. Incident analysis: Investigation and identification of the root cause, scope, and extent of the incident, will be carried out using tools such as logs, forensics, or malware analysis.

4.3.6. Incident eradication: Traces of the incident will be removed from the college's systems through methods such as deleting malicious files, patching vulnerabilities, or changing passwords.

4.3.7. Incident recovery: Normal operations and functionality will be reinstated through reinstallation of software, testing of systems, or updating of policies.

4.3.8. Incident documentation: Recording of all the actions taken during the incident response process, including the date, time, personnel involved, evidence collected, and lessons learned.

4.3.9. Incident review: Evaluation of the effectiveness of the incident response plan and identification of any gaps or areas for improvement. The plan will be updated accordingly, and regular training and testing conducted.

5. User Awareness and Training:

5.1. CRC's IT department is responsible for providing guidance and support to users on how to use IT and cyber security resources safely and effectively.

5.2. CRC promotes IT and cyber security awareness among all users through informational materials such as posters, messaging, newsletters and blog posts, regular training, and educational programs.

5.3. CRC's IT and cyber safety user awareness and training includes:

5.3.1. Promoting responsible online behaviour, safe browsing, and secure password practices.

5.3.2. Educating users about phishing, social engineering, and other common cyber threats.

5.3.3. Providing resources, such as guidelines, best practices, and reporting procedures.
5.3.4. Conducting periodic security awareness campaigns and assessments.

6. Compliance and Governance:
   6.1. CRC is committed to complying with applicable laws, regulations, and industry standards regarding cyber security and data protection. CRC therefore reserves the right to monitor, audit and investigate the use of its IT and cyber security resources to ensure compliance with this policy and other applicable policies, laws, and regulations.
   6.2. This policy will be reviewed and updated by CRC's administration at least annually or as necessary to reflect changes in technology, threats, and regulations. Any changes to this policy will be communicated to users through appropriate channels. Users are expected to always comply with the latest version of this policy.
   6.3. CRC designates the IT Manager and Head of Compliance as responsible individuals to monitor compliance with this policy and relevant regulations.

7. Policy Enforcement:
   7.1. CRC reserves the right to take appropriate disciplinary actions against any users who violate this policy or abuse their privileges. Such actions may include warnings, revoking access rights, suspending, or terminating accounts, imposing fines or sanctions, reporting to law enforcement authorities or taking legal actions.
   7.2. All users are responsible for reporting any suspected or observed policy violations to the appropriate authorities.
   7.3. The college administration will conduct periodic audits and assessments to ensure policy compliance and may take necessary actions based on the findings.
   7.4. CRC's IT department is responsible for implementing and enforcing this policy in collaboration with other relevant units and stakeholders.

Users are responsible for familiarising themselves with this policy and following its requirements. Users are also encouraged to seek advice from CRC's IT department or other experts if they have any questions or concerns regarding IT, AI, or cyber security issues.

By adhering to this policy, Christ The Redeemer College aims to create a secure and resilient environment that protects its information assets, promotes responsible behaviour, and mitigates the risks associated with cyber threats.