CATHOLIC EDUCATION
Archdiocese of Canberra & Goulburn
Catholic Archdiocese of Canberra and Goulburn Education Limited | ABN 60 675 797 734

CECG Vulnerability Disclosure Policy

Purpose

Catholic Education, Archdiocese of Canberra and Goulburn (CECG) welcomes feedback from security researchers and the general public to help improve our security. If you believe you have discovered a vulnerability, we want to hear from you.

The security researcher community makes valuable contributions to the security of an organisation and we are motivated to maintain a good relationship with this community. Such research will be viewed as a collaboration if security vulnerabilities are reported to us in accordance with this policy. In the event that a security vulnerability is not reported in accordance with this policy, we reserve all of our legal rights.

Systems in Scope

Our Vulnerability Disclosure policy applies to independent security researchers for any digital assets, systems, or Software as a Service (SaaS) cloud services provided by, or through CECG.

Note, this does not authorise you to conduct security testing against our systems. If you think a vulnerability exists, report it to us so that we can test and verify it.

Out of Scope

Assets or other equipment not owned by parties participating in this policy are out of scope. Vulnerabilities discovered or suspected in out-of-scope systems should be reported to the appropriate vendor or applicable authority.

For the avoidance of doubt, the following list includes, and is not limited to types of techniques that are not permitted during research activities:

- Actions that violate Australian law.

- Clickjacking.
- Social Engineering or phishing.
- Weak or insecure SSL ciphers or certificates.
- Denial of Service (DoS), or Distributed Denial of Service (DDoS) attacks.
- Physical attacks.
- Attempts to modify or destroy data.

Our Commitment

When working with us, according to this policy, you can expect us to:

- Respond to your report promptly, and work with you to understand and validate your report;
- Strive to keep you informed about the progress of a vulnerability as it is processed;
- Work to remediate discovered vulnerabilities in a timely manner, within our operational constraints.

When a report is made for a new vulnerability, we ask that you keep the information confidential and do not make your research public until we have completed our investigation and where applicable, have remediated or mitigated the vulnerability.