POLICY: Information Security

1. PURPOSE

The purpose of this policy is to describe Brisbane Catholic Education's (BCE) approach to managing BCE's internal information technology (IT) environment.

This policy must be read in conjunction with: Acceptable Use policy; Risk Management policy; and Catholic Education Archdiocese of Brisbane Code of Conduct.

2. RATIONALE

The BCE IT and business environment is intrinsically vulnerable to unauthorised or inappropriate use or release, accidental or deliberate damage and loss. Inappropriate use compromises the underlying data, the resultant information assembled, decision making, and the reputation of BCE.

3. POLICY STATEMENT

The security of BCE's IT resources is the responsibility of all users, including employees, students, parents, guardians, volunteers, and contractors. Information security is a governance process that seeks to minimise risks to BCE processes and to users of BCE's IT resources.

4. PRINCIPLES

BCE promotes a secure internal IT environment by applying the following principles:

- confidentiality: ensuring that information is accessible only to authorised users and privacy is maintained
- integrity: safeguarding and securing information, records, and critical applications
- continuity: owners of critical processes have access to IT resources
- compliance: ensuring that BCE systems, applications and processes meet due diligence requirements and comply with standards and procedures. This includes systems and applications used in schools.
- risk-based: evaluating threats, protect IT resources, promote a security-positive culture and encourage use that is ethical, responsible and lawful
- performance: providing timely and accurate information on information security performance to leadership and promote continuous improvement.

5. REFERENCES

- Acceptable Use policy
- Catholic Education Archdiocese of Brisbane Code of Conduct
- Risk Management policy.