POLICY: Information Security

1. PURPOSE

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

This policy must be read in conjunction with: IT Acceptable Use policy; Risk Management policy and Code of Conduct.

2. RATIONALE

BCE's IT and business environments are intrinsically vulnerable to unauthorised or inappropriate use, release, accidental or deliberate damage and loss. Improper 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 staff, students, parents, guardians, volunteers and contractors. Information security is a governance process that seeks to minimise risks to BCE processes and users of BCE's IT resources.

4. PRINCIPLES

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

- confidentiality: ensuring that information is accessible only to authorised users
- integrity: safeguarding and securing information, data, records and critical applications
- continuity: owners of critical processes have access to IT resources
- 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

- IT Acceptable Use policy
- Risk Management policy
- Code of Conduct.