ST JOSEPH'S PRIMARY SCHOOL

544 Balcombe Road, Black Rock, Vic 3193

Telephone: 9589 4685 Fax: 9589 7612

Email: office@sjblackrock.catholic.edu.au

www.sjblackrock.catholic.edu.au

Cybersafety Policy

Rationale

St Joseph's Catholic Primary School recognises the importance of teachers, students and parents engaging, collaborating, learning and sharing through Digital Technologies.
Our vision is to use technology to create an inclusive, safe and stimulating environment that promotes collaboration between students, teachers and parents to facilitate 21st century learning. By understanding and working with digital technologies, students acquire the knowledge, skills and personal qualities that enable them to communicate, view and listen safely and critically in an increasingly digital world.

St Joseph's has an obligation to maintain a safe physical and emotional environment, and a responsibility to consult with the community. These responsibilities are increasingly being linked to the use of the Internet and Information Communication Technologies (ICT), and a number of related cybersafety issues. The Internet and ICT devices/equipment bring great benefits to the teaching and learning programmes, and to the effective operation of the school.

However, we recognise that the presence in the learning environment of these technologies provided by the school, can also facilitate anti-social, inappropriate, and even illegal, material and activities. The school has the dual responsibility to maximise the benefits of these technologies, while at the same time to minimise and manage the risks.

St Joseph's School acknowledges the need to have in place rigorous and effective school cyber safety practices, which are directed and guided by this cyber safety policy.

Policy

St Joseph's will develop and maintain rigorous and effective cybersafety practices which aim to maximise the benefits of the internet and use of ICT devices/equipment for the effective operation of the school in student learning and, minimise and manage risks.

These cyber safety practices will aim to address the needs of students and other members of the school community to receive education about the safe and responsible use of current and developing information and communication technologies.

Policy Guidelines

Associated issues the school will address include:

- the need for on-going funding for cybersafety practices through the annual budget.
- the review of the Annual Action Plan and School Improvement Plan.

- the deployment of staff for professional development and training.
- implications for the design and delivery of the curriculum.
- the need for regular relevant education about cybersafety for the school community.
- disciplinary responses appropriate to breaches of cyber safety.
- the availability of appropriate pastoral support.
- potential employment issues.

To develop a cybercafé school environment, the Parish Priest will delegate to the principal the responsibility to achieve this goal by developing and implementing the appropriate management procedures, practices, electronic systems, and educational programmes.

22/3/2017

Guidelines for St Joseph's cyber safety practices

1. The school's cybersafety practices are to be based on information from the Office of the E-Safety Commissioner and child safety policy
2. No individual may use the school Internet facilities and school-owned/leased ICT devices/equipment in any circumstances unless the appropriate use agreement has been signed and returned to the school. Use agreements also apply to the use of privately-owned/leased ICT devices/equipment on the school site, or at/for any school-related activity, regardless of its location. This includes off-site access to the school network and/ or cloud based drives from school or privately-owned/leased equipment.
3. St Joseph's use agreements will cover all board employees, all students (including adult and community), and any other individuals authorised to make use of the school Internet facilities and ICT devices/equipment, such as teacher trainees, external tutors and providers, contractors, and other special visitors to the school.
4. The use agreements are also an educative tool and should be used as a resource for the professional development of staff.
5. Use of the Internet and the ICT devices/equipment by staff, students and other approved users at St Joseph's is to be limited to educational, professional development, and personal usage appropriate in the school environment, as defined in individual use agreements anad child safety policy..
6. Signed use agreements will be filed in a secure place, and an appropriate system devised which facilitates confirmation that particular individuals are authorised to make use of the Internet and ICT devices/equipment.
7. The school has the right to monitor access and review all use. This includes personal emails sent and received on the school's computer/s and/or network facilities at all times.
8. The school has the right to audit at anytime any material on equipment that is owned or leased by the school. The school may also request permission to audit privately owned ICT devices/equipment used on the school site or at any school related activity.
9. Issues relating to confidentiality, such as sighting student or staff information, reasons for collecting data and the secure storage of personal details and information (including images) will be subject to the provisions of the Privacy Act .
10. The safety of children is of paramount concern. Any apparent breach of cybersafety will be taken seriously. The response to individual incidents will follow the procedures developed as

part of the school's cybersafety practices. In serious incidents, advice will be sought from an appropriate source.

11. There will be special attention paid to the need for specific procedures regarding the gathering of evidence in potentially serious cases. If illegal material or activities are suspected, the matter may need to be reported to the relevant law enforcement agency.

Date for review: 2012, 2016