

# St Philip's Blackburn North



## CYBERSAFETY POLICY

### VISION AND MISSION

#### Vision Statement

**Modelling the teachings of Christ,  
St Philip's School community aspires to be a place of welcome that provides many  
learning environments to meet the challenges of an ever-changing world.**

#### Mission Statements

Because we believe that Christ is the central focus of our school and we are witnesses to him and his teachings we aim to:

- provide an atmosphere where all are made welcome, where they feel safe and have a sense of belonging
- provide a school environment that is positive and challenges all students to work to the best of their ability
- foster in all a realisation that they are responsible for their own learning
- develop a sense of justice by respecting the opinions and rights of others
- encourage all to be sensitive to others and respect their differences
- encourage all to use their physical environments in a respectful manner
- provide a learning environment that utilises the most effective and current approaches in education.

#### RATIONALE

The overall goal of St Philip's Primary School is to create and maintain a cybersafety culture that is in keeping with our values and with legislative and professional obligations. This policy is aligned with other Wellbeing and Digital policies. The Acceptable Use Agreement for staff and students outlines the obligations, responsibilities and the nature of possible consequences associated with cybersafety breaches that undermine the safety of members of the school community and beyond.

Digital equipment/devices bring great benefits to the teaching and learning programmes at St Philip's and to the effective operation of the school. The equipment is for educational purposes appropriate to this environment.

#### DEFINITIONS

**Cybersafety** refers to the safe use of the Internet and equipment/devices, including mobile phones.

## St Philip's Blackburn North

**Cyberbullying** is bullying which uses e-technology as a means of victimising others. It is the use of an internet service or mobile technologies, including social networking services eg. Instant messaging, Facebook, Twitter etc. with the intention of harming another person.

**Digital Technologies** refers to the school's computer network, internet access facilities, computers and other equipment/devices as outlined below.

**Equipment/devices** includes computers such as desktops, Chrome Books, laptops and iPads, storage devices such as USBs, CDs, DVDs and audio players, cameras, mobile phones and any other similar technologies.

**Inappropriate material** means material that deals with matters such as inappropriate language, images or information.

**E-crime** occurs when computers or other electronic communication equipment/devices are used to commit an offence.

### IMPLEMENTATION

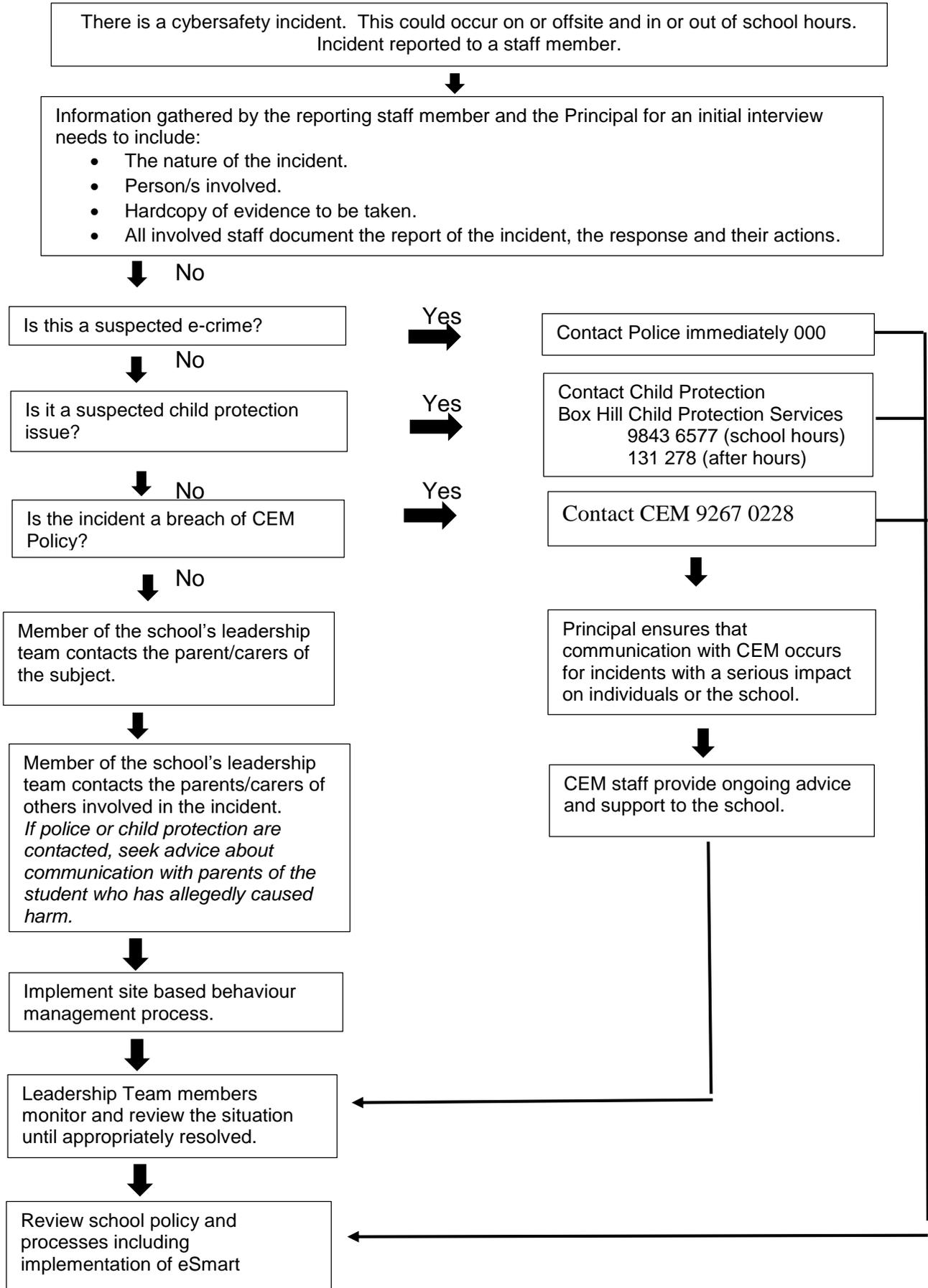
The measures to ensure the cybersafety of students and staff are based on our school values of Respect for Self, Others and the Environment. All students will be issued with an annual user's agreement and once signed consent has been returned to the school, students will be able to use the school's digital devices.

Rigorous cybersafety practices are in place which include the annual cybersafety agreement for staff and students. Child protection education and eSmart protection curriculum includes information about remaining safe when using technologies and is provided to staff, students and parents.

Material sent and received using the network may be monitored and filtered. Monitoring software may be used to restrict access to certain sites and data, including email. Where a student is suspected of a cybersafety incident the St Philip's Cybersafety Action Flow Chart is to be used.

# St Philip's Blackburn North

## St Philip's School Cybersafety Action Flow Chart



## St Philip's Blackburn North

### USEFUL WEBSITES:

**Esafety:** [www.esafety.gov.au](http://www.esafety.gov.au)

Cybersmart provides activities, resources and practical advice to help young children, children, teens and parents safely enjoy the online world. Developed by the Australian Communications and Media Authority, Cybersmart is part of the Australian Government's cybersafety programme.

**Alannah and Madeline Foundation:** [www.amf.org.au](http://www.amf.org.au)

The Alannah and Madeline Foundation's initiatives include eSmart for Schools and Libraries and the eSmart Digital Licences for students in the upper school.

**Cybersafety in Schools:** <https://www.education.gov.au/aus-student-wellbeing-framework>

This page from the Australian Government has a series of links for cybersafety and anti-bullying education.

**The Modern Parent:** [www.themodernparent.net](http://www.themodernparent.net)

Martine Oglethorpe is a cybersafety expert who has visited our school and this is her website.

**Cybersafety Solutions:** [www.cybersafetysolutions.com.au](http://www.cybersafetysolutions.com.au)

Susan McLean is a cybersafety expert. Her site offers a level of cyber assistance to parents, students and schools.

**NetSmartz:** [www.NetSmartz.com](http://www.NetSmartz.com)

Recommended by Susan McLean as excellent content. This is a programme from the USA.

**Bullying.org** [www.bullying.org](http://www.bullying.org)

Bullying.org's purpose is to prevent bullying in our society through education and awareness.

**i-SAFE** [www.iSafe.org](http://www.iSafe.org)

i-SAFE Inc. is a United States based leading publisher of media literacy and digital citizenship education materials and programming with worldwide distribution.

### Related Policies

Behaviour Management Policy

Child Safe Policy

Student Wellbeing Policy

Staff and Student Digital Technologies and User Agreements

Social Media Policy

Social Media for Staff Policy

# **St Philip's Blackburn North**

## **REVIEW**

Current Review: July 2019

Ratified by the Education Board: 10<sup>th</sup> September 2019

Next Review: July 2021