

## Cyber Safety Policy

---

### **The Hazard – Cyber Safety**

Cyber safety refers to the safe and responsible use of information and communication technologies. This includes privacy and information protection, respectful communication and knowing how to get help to deal with online issues.

#### **Common cyber safety issues include:**

Cyber bullying is the ongoing abuse of power to threaten or harm another person through the use of technology (Refer to our Bullying Prevention and Intervention Policy);

Sexting is the sending or posting of provocative or sexual photos, messages or videos online;

Identity theft is the fraudulent assumption of a person's private information for their personal gain. Students are exposed to these risks as they are often unaware of the safety issues surrounding their digital footprint; and

Predatory behaviour where a student is targeted online by a stranger who attempts to arrange a face to face meeting, in an attempt to engage in inappropriate behaviour.

Cyber safety issues most commonly occur through a student's use of their own technology devices (e.g. smart phone, tablet, laptop, home computer).

Safe use of technology whilst at school is managed through our Information and Communication Technology (ICT) Policy.

### **Firbank Grammar's Policy**

Firbank Grammar recognises its duty to students to provide a safe and positive learning environment which includes the responsible use of information and communication technologies.

It is our policy that:

- Cyber safety be managed through a 'whole of school community' approach involving students, staff and parents/carers;
- Cyber safety and cyber bullying prevention strategies be implemented within the school on a continuous basis with a focus on teaching age appropriate skills and strategies to empower staff, students and parents/carers to recognise cyber safety issues and respond appropriately;
- Cyber bullying response strategies be tailored to the circumstances of each incident; and
- Our bullying prevention, intervention and cyber safety strategies are reviewed on an annual basis against best practice.

### **Cyber Safety Strategies**

Firbank Grammar recognises that the implementation of whole school cyber safety strategies is the most effective way of minimising risks related to our students engaging in online activity.

The following initiatives form part of our overall cyber safety strategy within the school:

- Establishment of a 'Cyber Safety Team' and appointment of three primary 'Cyber Safety Contact Persons' (refer below for details);
- A structured curriculum, that provides age appropriate information and skills relating to cyber safety (including cyber bullying);
- Education, training and professional development of staff in cyber safety strategies;
- Regular provision of information to parents/carers to raise awareness of cyber safety as a school community issue;
- Promotion of a supportive environment that encourages the development of positive relationships and communication between staff, students and parents/carers;

## Cyber Safety Policy

---

- Promotion of responsible bystander behaviour amongst students, staff and parents/carers (this may occur where a bystander observes inappropriate online behaviour either being perpetrated by, or targeted at, a student);
- Reporting of cyber safety incidents is encouraged and made easy through the establishment of multiple reporting channels (as specified below);
- Regular risk assessments of cyber safety within the school are undertaken by surveying students to identify cyber safety issues;
- Records of reported cyber safety incidents are maintained and analysed, in order to identify systemic issues and to implement targeted prevention strategies where appropriate;
- Cyber safety strategies are included in students' school diaries;
- Cyber safety posters are displayed strategically within the school;
- Promotion of student cyber safety awareness by participating in relevant cyber safety related events; and
- Reporting procedures are available online for students.

### **Our Cyber Safety Team & Contact Person**

Firbank Grammar has established a Cyber Safety Team whose role it is to:

- Review the school's cyber safe policy and relevant cyber safety initiatives (such as student education, staff professional development, parent/carer information) on at least an annual basis to ensure that they are effective in minimising cyber safety risks within the school;
- Maintain up to date knowledge of cyber safety best practice for schools;
- Maintain up to date knowledge of available cyber safety resources that may be utilised by the school and/or integrated in the school's cyber safety program;
- Review and analyse data obtained from school surveys that deal with cyber safety issues;
- Conduct regular risk assessments with respect to cyber safety issues within the school;
- Make recommendations to the Principal with respect to improvements to the school's cyber safety policies and procedures; and
- Appoint a member who shall be the primary point of contact for cyber safety related issues that may arise during the year.

### **Current members of the Cyber Safety Team are as follows:**

The Heads of Campus (Turner House, Sandringham and Senior School)

School Psychologists, representative from IT Department

The Cyber Safety Team meets each semester.

## Cyber Safety Policy

---

The Heads of Campus are the 'Cyber Safety Primary Contacts'.

Wellbeing Leaders in Senior School may also act as a primary point of contact and will liaise with the Heads of Campus who are put forward to the school community as the first contact point for students, staff and parents if a cyber safety issue arises.

Cyber Safety Primary Contacts are encouraged to attend relevant external cyber safety training programs.

### **Staff Responsibility**

All staff are responsible to:

- Model appropriate online behaviour at all times;
- Refer any cyber safety related issues to the Cyber Safety Primary Contacts; and
- Acknowledge the right of parents to speak with school authorities if they believe their child is at risk.

### **Implementation**

This policy is implemented through a combination of:

- Staff training;
- Student and parent/carer education and information;
- Effective incident reporting procedures;
- Effective management of cyber safety incidents when reported;
- The creation of a zero tolerance 'no bullying' culture within the school community;
- Effective record keeping procedures;
- Initiation of corrective actions where necessary; and
- Promotion of respectful relationships

### **Discipline for Breach of Policy**

Where a staff member breaches this policy Firbank Grammar will take appropriate disciplinary action.

### **Related Policies**

- Bullying Prevention and Intervention Policy
- Technology Policy