

# CYBERSAFETY AT HOWICK PRIMARY SCHOOL

## SECTION A – CYBERSAFETY AND THE SCHOOL COMMUNITY

### **- THE ROLE OF USE AGREEMENTS IN THE HOWICK PRIMARY SCHOOL CYBERSAFETY PROGRAMME -**

The values promoted by HPS include [respect for self and all others in the school community, and commitment to enabling everyone to achieve their personal best in an environment which is physically and emotionally safe]. The measures to ensure the cybersafety of the school environment which are outlined in this document are based on these core values.

The school's computer network, Internet access facilities, computers and other school ICT equipment/devices bring great benefits to the teaching and learning programmes at HPS, and to the effective operation of the school. (Examples of what is meant by 'ICT equipment/devices' can be found on the cover page.) However, it is essential that the school endeavours to ensure the safe use of ICT within the school community.

*Thus HPS has rigorous cybersafety practices in place, which include cybersafety use agreements for all school staff and students.*

Cybersafety use agreement documents include information about obligations and responsibilities, and the nature of possible consequences associated with breaches of the use agreement which undermine the safety of the school environment. The cybersafety education supplied by the school to its learning community is designed to complement and support the use agreement initiative. The overall goal of the school in this matter is to help keep the school community cybersafe by creating and maintaining a cybersafety culture which is in keeping with the values of the school, as well as legislative, and professional, obligations. All members of the school community benefit from being party to the use agreement initiative and other aspects of the school cybersafety programme.

**Some of the information in this section is less likely to apply to young children while at school, however it is helpful for parents to be aware of the scope of this important, school-wide, cybersafety initiative. It also provides parents with valuable educative material to assist them in their efforts to keep their children cybersafe.**

#### **1. Cybersafety use agreements**

- 1.1. All staff and students, whether or not they presently make use of school ICT, will be issued with a use agreement. Parents are required to read these pages carefully, and return the signed use agreement form in Section B to the school office for filing.
- 1.2. Parents are asked to keep the other pages of the agreement for later reference. (If necessary, a replacement copy will be supplied by the school's Cybersafety Manager.)
- 1.3. The school encourages anyone with a query about the agreement to contact the Cybersafety Manager or the Principal as soon as possible.

#### **2. Requirements regarding appropriate use of ICT in the school learning environment**

In order to meet the school's legislative obligation to maintain a safe physical and emotional learning environment, and be consistent with the values of the school:

- 2.1. The use of **the school's** computer network, Internet access facilities, computers and other school ICT equipment/devices, on or off the school site, is limited to educational purposes appropriate to the school environment. This applies whether or not the ICT equipment is owned/leased either partially or wholly by the school. If any other use is permitted, the user(s) will be informed by the school.
- 2.2. The school has the right to monitor, access, and review all the use detailed in 2.1. This includes personal emails sent and received on the school's computers and/or network facilities, either during or outside school hours.
- 2.3. The use of any **privately-owned/leased** ICT equipment/devices on the school site, or at any school-related activity, must be appropriate to the school environment. This includes any images or material

present/stored on privately-owned/leased ICT equipment/devices brought onto the school site, or to any school-related activity.

Such equipment/devices could include a laptop, desktop, PDA, mobile phone, camera, recording device, or portable storage (like a USB or flash memory device). Anyone unsure about whether or not it is appropriate to have a particular device at school or at a school-related activity, or unsure about whether the planned use of a particular device is appropriate, should check with the IT Manager. For students, it is appropriate they check with their teacher.

*Note that examples of a 'school-related activity' include, but are not limited to, a field trip, camp, sporting or cultural event, wherever its location.*

- 2.4. **When using a global information system** such as the Internet, it may not always be possible for the school to filter or screen all material. This may include material which is **inappropriate** in the school environment (such as 'legal' pornography), **dangerous** (such as sites for the sale of weapons), or **illegal** (which could include material defined in the Films, Videos and Publications Classification Act 1993, such as child pornography; or involvement with any fraudulent activity).

*However, the expectation is that each individual will make responsible use of such systems.*

### 3. Monitoring by the school

- 3.1. HPS has an electronic access monitoring system which has the capability to record Internet use, including the user details, time, date, sites visited, length of time viewed, and from which computer or device.
- 3.2. The school monitors traffic and material sent and received using the school's ICT infrastructures. From time to time this may be examined and analysed to help maintain a cybersafe school environment.
- 3.3. The school will deploy filtering and/or monitoring software where appropriate to restrict access to certain sites and data, including email.

*However, as in 2.4., the expectation is that each individual will be responsible in their use of ICT.*

### 4. Audits

- 4.1. The school will from time to time conduct an internal audit of its computer network, Internet access facilities, computers and other school ICT equipment/devices, or may commission an independent audit. If deemed necessary, auditing of the school computer system will include any stored content, and all aspects of its use, including email. An audit may also include any laptops provided or subsidised by/through the school or subsidised by a school-related source such as the Ministry of Education.

### 5. Breaches of the use agreement

- 5.1. Breaches of the use agreement can undermine the values of the school and the safety of the learning environment, especially when ICT is used to facilitate misconduct.
- 5.2. Such a breach which is deemed harmful to the safety of the school (for example, involvement with inappropriate material, or anti-social activities like harassment), may constitute a significant breach of discipline and possibly result in serious consequences. The school will respond to any breach of the use agreement in an appropriate manner, taking into account all relevant factors, including contractual and statutory obligations.
- 5.3. If there is a suspected breach of use agreement involving privately-owned ICT on the school site or at a school related activity, the matter may be investigated by the school. The school may request permission to audit that equipment/device(s) as part of its investigation into the alleged incident.
- 5.4. Involvement with **material** which is deemed 'age-restricted', or 'objectionable' (illegal), under the Films, Videos and Publications Classification Act 1993, is a very serious matter, as is involvement in an **activity** which might constitute criminal misconduct, such as harassment. In such situations, it may be necessary to involve law enforcement in addition to any disciplinary response made by the school as a result of its investigation.

### 6. Other aspects of the school's cybersafety programme

The use agreements operate in conjunction with other cybersafety initiatives, such as cybersafety education supplied to the school community. This education plays a significant role in the school's overall cybersafety programme, and also helps keep children, young people and adults cybersafe in all areas of their lives. If more information is required, the Cybersafety Manager, or the Principal, can be contacted.