Harrytown Catholic High School
Staff Acceptable Use Agreement for the Internet, Email and Other Technologies

The computer system is owned by the School and is made available to staff to enhance their professional activities including teaching, training, research, administration and management. The equipment supplied to staff is for their use and not the use of their families.

This agreement has been drawn up to protect staff and the school. By logging onto School IT equipment, staff agree to adhere to this policy.

Network Security

- All computer users must log onto the system using their own allocated usernames and passwords and must not use those allocated to other staff.
- Passwords must be kept secure and never written down; care should be taken when entering your password where others are nearby who may be able to view it.
- PCs and Laptops should be locked when left unattended. This is done by pressing <Ctrl><Alt><Delete> and choosing "Lock this computer".
- The School reserves the right to examine or delete any files held on its computer system.
- Staff are not allowed to use schools computers for any form of illegal activity for example, downloading Copyright material, introducing viruses or hacking into other computers (Computer Misuse Act 1990; Data Protection Act).
- Users must not wilfully make any changes to computer settings, delete any software or interfere with another person's work files.
- Permission must be obtained from the IT Manager before any software is installed or downloaded from the Internet.
- Staff must take all reasonable steps to ensure that material brought in from home is virus free.
- Staff are responsible for any equipment belonging to the School which is taken off site.
- Staff are not permitted to bring in their own devices from home and place them on the School network.
- Any document containing student data must be password protected using the standard school password.
- Photographs of children must not be taken on members of staffs personal cameras or mobile phones. In addition, all photographs taken on school equipment must be removed from the device and stored on the server as soon as possible.

Internet Security

- The school reserves the right to examine and monitor any Internet Sites visited.
- Viewing or downloading offensive or any other inappropriate material from any source is forbidden. The storing of such images or text using school equipment is also forbidden.
- Anyone inadvertently accessing inappropriate material should immediately inform the IT Manager and ensure that the incident is recorded. Your report will be treated confidentially.
- All Internet activity undertaken in teaching hours will be appropriate to staff's professional use or the student's education.
- Access to staffs personal social media accounts at School is prohibited. This includes, but is not limited to Facebook and Twitter.

Social Networking and Implications for School Staff

- Reference to school
- Reference to individuals related to school
- Contact with pupils including past pupils
- Reference to Teachers' standards
- Reference to Code of Conduct

Email Security

- The school reserves the right to examine all emails exchanged using a School email address.
- The sending of abusive or other offensive Email using school facilities is likely to be considered a criminal act
- Users are responsible for all Email sent and received, including from newsgroups, and will be vigilant about the risk of virus infection from files attached to Emails.
- The same professional levels of language and content should be applied to Email as for letters or other media.

Mobile Phones

- If you need to be contacted urgently during the school day then this should be done via the school office. The use of mobile telephones in the classroom or other working environment, e.g. Office, or whilst on duty, is not permitted and leaving the room to take such a call is not appropriate.
- If you are required to take an urgent call then the school receptionist will liaise with Cover and/or SLT to arrange for someone to come and take over your teaching whilst you take any call of this nature.
- If you have a mobile telephone which is switched on in school you should be aware of having it protected so that it is not visible to others via Bluetooth. You should not accept any data transmitted to you via Bluetooth whilst at school as it may well compromise your safety.
- Occasionally it is necessary for professional academic reasons for staff to communicate with students/pupils out of school. Personal email addresses, home or mobile phone numbers should not be given, asked for or used. During an educational visit; the school's mobile phone should be used for contacting pupils and / or parents. Pastoral matters should not normally be dealt with by personal email or using personal phone contacts. Only in the most exceptional circumstances, for instance, where there is well-founded concern for the unexplained whereabouts of a student, should pastoral matters be dealt with by personal email or using personal phone contact. In any event, records of all contacts should be kept on the student file so that if it is necessary to use email or personal contact, the reason why will be specified in the written record. It is very difficult to envisage circumstances under which individual texting is appropriate except through official school channels. On any occasion where you contact pupils or parents using your own personal phone, you should hide your outgoing number by prefacing the number dialled with 141 for landlines or #31# for mobile phones, (every carrier is different, so if #31# doesn't work, try one of the following number/symbol combinations before entering the number you're calling: *#30# / *#31# / *31#.)

Declaration

- I understand the terms used in this acceptable use policy and agree to follow the guidelines accordingly. I understand that any breach of the above agreement, depending on the seriousness of the situation, could lead to action being taken under the school's disciplinary policy.
