Acceptable Use (students)

POLICY

Rationale:

Guidelines and Conditions for Appropriate Use of ICT facilities

The Derrimut Primary network is provided for staff and students to promote educational excellence by facilitating resource sharing, innovation and communication.

Aims:

- All students are given full access to the network with a class account. Students also have full Internet access for the purposes of learning. Any such facilities must be regarded as privileges, which may be withdrawn for misuse of the resources.
- Computing facilities are provided primarily for the educational benefit of students and the professional development of staff. Any behaviour that interferes with these primary objectives will be considered an infringement of Acceptable Use.

Implementation:

1. General Policies

- Use of ICT/internet resources for educational purposes has priority over other (recreational) uses
- Appropriate language must be in all communications including email messages, social media, chat and web pages
- No user may deliberately or carelessly waste ICT resources (e.g. unnecessary printing) or disadvantage other users (eg by monopolising equipment, network traffic etc).

Students must not:

- Use abusive or obscene language in any communications
- Steal, or deliberately or carelessly cause damage to any equipment
- Interfere with or change any software settings or other people's files
- Attempt to get around or reduce network security
- Do anything in any other person's home directory and online environment
- Store unauthorised types of files in their own home directories
- Waste resources
- Send "spam" (bulk and/or unsolicited e-mail)
- Reveal personal information in any communications
- Deliberately enter, or remain in, web sites containing objectionable material
- Knowingly infringe copyright

2. ICT hardware

ICT facilities are expensive, sensitive and must be treated carefully. Students must not:

- Do anything likely to cause damage to any equipment, whether deliberately or carelessly
- Steal equipment
- Vandalise equipment (e.g. graffiti)
- Mark or deface any equipment
- Interfere with networking equipment such as hubs
- Eat or drink near any School owned ICT resources

Students must not, without permission:

- Attempt to repair equipment without permission
- Unplug cables or equipment
- Move equipment to another place
- Remove any covers or panels
- Disassemble any equipment
- Disable the operation of any equipment

Students must also report other people breaking these rules.

Regardless of the real or supposed levels of understanding, students are NOT authorised to attempt the repair or adjustment of any school hardware or software. Any such attempt will be regarded as a violation of network security. Any problem with equipment or software must be referred to an authorised person.

3. Software and operating systems

ICT operating systems and other software must be set up properly for ICTs to be useful.

Students will not:

- Change any ICT settings (Airwatch desktops, menus standard document settings etc) without permission

- Bring or download unauthorised programs, including games, to the school or run them on school ICTs.
- Delete, add or alter any configuration files
- Copy any copyrighted software to or from any ICT, or duplicate such software
- Deliberately introduce any virus or program that reduces system security or effectiveness
- Create copies of, or modify files or other data or passwords belonging to other users.

5. Printing
Students must minimise printing at all times by print previewing, editing on screen rather than on printouts and spell-checking before printing.

Students must not load paper into printers without permission.

6. Internet usage
Internet access is expensive and has been provided to assist students' education. Students must use it only with permission, and not in any unauthorised way. It is not intended for entertainment.

Internet usage by students should be supervised by teachers and parents. Students should invoke protocols of switching off the screen and informing an adult if they access inappropriate content. To end, filtering software has been placed on the school online portal. In the end, however, it is the responsibility of individual students to ensure their behaviour does not contravene school rules or rules imposed by parents/ guardians.
The school is aware that definitions of "offensive" and "inappropriate" will vary considerably between cultures and individuals. The school is also aware that no security system is perfect and that there is always the possibility of inappropriate material, intentionally and unintentionally, being obtained and displayed.

It is the responsibility of the school to:-
- provide training on the use of the Internet and make that training available to everyone
- take action to block the further display of offensive or inappropriate material that has appeared on the Internet links

The Internet is a vast source of material of all sorts of quality and content. The school will exercise all care in protecting students from offensive material, but the final responsibility must lie with students in not actively seeking out such material.
It is conceivable that, especially for senior students, information is required for curriculum purposes that may appear to contravene the following conditions. In such cases, it is the responsibility of students and teachers to negotiate the need to access such sites.

- Students will not deliberately enter or remain in any site that has any of the following content:
    - Nudity, obscene language or sexual discussion intended to provoke a sexual response
    - Violence
    - Information on, or encouragement to commit any crime
    - Racism
    - Information on making or using weapons, boobytraps, dangerous practical jokes or "revenge" methods
    - Any other material that the student's parents or guardians have forbidden them to see
- If students encounter any such site, they must immediately turn off the ICT monitor (iPad screen) (not the ICT itself) and notify a teacher. Do not show your friends the site first.
- The Internet must not be used for commercial purposes or for profit.
- The Internet must not be used for illegal purposes such as spreading ICT viruses or distributing/receiving software that is not in the public domain.
- It is inappropriate to act as though you intend to break the law e.g. by attempting to guess a password or trying to gain unauthorised access to remote ICTs. Even if such attempts are not seriously intended to succeed, they will be considered serious offences.
- Interactive use of the Internet should ensure that there is no possibility of the transmission of viruses or programs which are harmful to another user's data or equipment.
- Copyright is a complex issue that is not fully resolved as far as the Internet is concerned. It is customary to acknowledge sources of any material quoted directly and it is a breach of copyright to transmit another user's document without their prior knowledge and permission. This includes the use of images and text. It is safest to assume all content on web sites is the legal property of the creator of the page unless otherwise noted by the creator.

7. Possible consequences
More than one may apply for a given situation. Serious or repeated incidences of misuse offences will result in stronger consequences.
- Removal of internet access privileges
- Reflection Time
- Paying to replace damaged equipment
- Suspension

Evaluation:
* This policy will be reviewed as part of the school’s three-year review cycle.
* This policy was last ratified by School Council on 8/12/15

Updated December 2015 Version 1.2