EAST AYRSHIRE COUNCIL

Economy and Skills – Education Department

ACCEPTABLE USAGE OF COMPUTER FACILITIES - POLICY FOR STUDENTS

AUGUST 2019

Guidelines and Conditions for Appropriate Use of Computer Facilities

1. INTRODUCTION

The school network is provided to promote educational excellence by facilitating resource sharing, innovation and communication. All secondary students are given access to the network with an individual account including Internet access, primary school pupils are given the use of computers with internet access. Any such facilities must be regarded as privileges which may be withdrawn for misuse of the resources.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. Any behaviour that interferes with these primary objectives will be considered an infringement of Acceptable Use.

2. GENERAL POLICIES

- Appropriate language must be used in all communications including email messages, chat and web pages
- No user may deliberately or carelessly waste computer resources (eg unnecessary printing) or disadvantage other users (e.g. by monopolising equipment, network traffic etc).
- Consideration must be given to avoiding inconvenience to other computer users. e.g. use headphones to listen to sound or music; leave computers ready for the next user to log in; not leave programs running on computers when you leave.

3. COMPUTER HARDWARE

Computer 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
- Vandalise equipment (e.g. graffiti)
- Mark or deface any equipment
- Interfere with equipment
- Eat or drink near any computer resources

Students must not, 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

4. SOFTWARE AND OPERATING SYSTEMS

Computer operating systems and other software must be set up properly for computers to be useful. Students must not:

- Change any computer settings (including screen savers, wallpapers, desktops, menus standard document settings etc) without permission
- Bring or download unauthorised programs, including games, to school or run them on school computers. Non-educational online internet games are banned
- Delete, add or alter any configuration files
- Copy any copyrighted software to or from any computer, or duplicate such software
- Deliberately introduce any virus or program that reduces system security or effectiveness

5. NETWORKS

Network accounts are to be used only by the authorised owner of the account. If you find a computer logged in, you should do nothing in that account except log out.

Students must not:

- Attempt to log into the network with any user name or password that is not their own, or change any other person's password
- Reveal their password to anyone except the system administrator or classroom teachers, if necessary. Students are responsible for everything done using their accounts, and everything in their home directories.
- Use or possess any program designed to reduce network security including but not limited to key logging software
- Enter any other person's home directory (drive H:) or do anything whatsoever to any other person's files
- Intentionally seek information on, obtain copies of, or modify files, other data or passwords belonging to other users
- Attempt to alter any person's access rights, including there own
- Store the following types of files in their home directory, without permission:
    - Program files (EXE, COM)
    - Compressed files (ZIP, ARJ, LHZ, ARJ, TAR etc)
    - Picture files, unless they are required by a subject
    - Sound/Music files (WMA, MP3, AIF etc) , unless they are required by a subject
    - Obscene material – pictures or text
    - Files with obscene filenames
    - Insulting material
    - Password-protected files
    - Copyrighted material.

6. INTERNET USAGE

6.1 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. It should be noted that access to the internet is logged, allowing reports to be created indicating which sites have been visited and by whom. These reports are available to Head Teachers and Heads of Service.

Because the Internet is an environment which is not policed, the school has a responsibility to ensure that, as far as possible, material obtained from the Internet is not offensive or inappropriate. To this end, filtering software has been placed on the Internet links. 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.

6.2 World Wide Web

The World Wide Web is a vast source of material of all sorts of quality and content. The council 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, booby-traps, dangerous practical jokes or "revenge" methods
- Proxy avoidance
- Any other material that the student's parents or guardians have forbidden them to see

If students encounter any such site, they must immediately notify a teacher. They should not show their 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 computer 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 computers. 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.

6.3 Email

Electronic mail is a valuable tool for communication. Students are encouraged to use it and take advantage of its special features. As with all privileges its use involves responsibilities.

Throughout the Internet there are accepted practices known as Netiquette which should be followed. The following points should be noted:

- Use appropriate language and be polite in your messages. Do not be insulting, abusive, swear or use vulgarities.
- Hate mail, chain letters, harassment, discriminatory remarks and other antisocial behaviours should never be written. Therefore no messages should contain obscene comments, threats, sexually explicit material or expressions of bigotry or hate.
- Do not reveal your personal details.
- Note that email is not guaranteed to be private. System administrators do have access to all files including mail. Messages relating to illegal activities may be reported to the authorities.

Students will not:

- send offensive mail
- send unsolicited mail to multiple recipients ("spam")
- use email for any illegal, immoral or unethical purpose
- attempt to disguise their identity or the true origin of their mail
- forge header messages or attempt to use any mail server for deceptive purposes
- use any mail program designed to send anonymous mail

If a student receives an inappropriate e-mail they should notify a member of staff.

6.4 Chat (IRC, MSN Messenger, ICQ etc)

Real-time chat programs are **not** to be used by students unless instructed by a teacher.

6.5 Access to Glow

Glow is an online resource that is being setup by the Scottish Executive in conjunction with Learning teaching Scotland and all 32 councils. It is envisaged that students will have access to this both in school and out with school. Students use of this resource is covered by this policy. Any breach of this policy will be treated as if the breach had occurred in school and may result in access to GLOW being withdrawn.

6.6 Summary of conditions

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
- Use proxy avoidance systems or sites.
- Do anything in any other person's home directory
- 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

7. POSSIBLE SANCTIONS

More than one may apply for a given offence. Serious or repeated offences will result in stronger penalties.

- Ban on lunchtime computer use
- Temporary ban on using computers
- Removal of email privileges
- Removal of internet access privileges
- Removal of home directory and network access (this may have the consequence of rendering the student unable to satisfactorily complete unit requirements of the subject)
- Detention
- Paying to replace damaged equipment
- Removal from classes where computer use is involved
- Exclusion from school
- Criminal charges

EAST AYRSHIRE COUNCIL

Economy and Skills - Education

Acceptable Usage of Computer Facilities Policy for Students

August 2019

Primary School Name : Catrine Primary School

Pupil Name (please print) _____

Class _____

I have read the East Ayrshire council acceptable use of computer facilities policy for students and discussed this with my child.

I agree/do not agree* to my son/daughter (named above) having access to computer facilities and internet related facilities based on this document.

Signature of parent/carer. _____

* please delete as appropriate