PRESTWICH ARTS COLLEGE

Statement of Policy on Acceptable Use of ICT Equipment and Related Electronic Communications STUDENTS

RATIONALE

Information and Communication Technology (ICT) prepares students to participate in a rapidly changing world in which work and other activities are increasingly transformed by access to varied and developing technology. Students use ICT tools to find, explore, analyse, exchange and present information responsibly, appropriately and safely. They learn how to employ ICT to enable rapid access to ideas and experiences from a wide range of people, communities and cultures. Increased capability in the use of ICT promotes initiative and independent learning; with students being able to make informed judgements about when and where to use ICT to best effect, and consider its implication for home and work both now and in the future.

AIMS

- To ensure students understand responsible use of ICT and related electronic communications
- To provide guidance in the use of ICT and related electronic communications
- To clarify correct and proper use of ICT
- To clarify what constitutes misuse of ICT and related electronic communications
- To promote the education of safe use of ICT and related electronic communications (e-safety)
- To promote confidence to deal with associated issues in an appropriate manner
- To support parents and carers to protect their children from the dangers of ICT misuse and related electronic communications
- To set out how e-safety will be taught across the school

PRACTICES

The Acceptable Use Policy applies to all users of Prestwich Arts College computer network and to the use of any of the School-owned computers, wherever they are physically located. The policy also applies whenever data is transmitted over the School's network via a privately-owned machine, wherever the machine is physically located.

Breaches of the Acceptable Use Policy are treated most seriously. Any such breach will be pursued by the Head of ICT who, along with the relevant Progress Manager, determine the appropriate sanctions.

These sanctions could include;

- Temporary or permanent ban on Internet use.
- Disciplinary action in line with existing practices and conditions of service.
- In extreme circumstances the Local Education Authority and / or the Police may need to be involved.

The school reserves the right, but not the duty, to monitor any and all aspects of its electronic resources and access to web sites, blogs and other accounts (eg twitter). The school also reserves the right to retrieve the contents of any student communication in these systems. This process is in place to maintain the integrity of the school's electronic systems, the rights of other users and to ensure compliance with the school's policies and obligations.

File Storage

Although the school makes every effort to ensure the integrity, security and back-up of data on the School network, users are advised to make sure they have a second copy (backup) of all their academic data. Pupils are advised early on to purchase a USB pen to assist in the protection against data loss.

All pupils have document network storage areas and an email inbox on the servers. In addition, shared work areas are available on the servers for pupils to access files. Any files which are deliberately stored on our servers in an area that is deemed contrary to its intended purpose may be deleted without notice by the Network Administrator.

Network Security

Throughout the system pupils must **NOT**:

- Use someone else's username or password to gain access to the school network, nor allow someone else to use your username or password
- Leave a PC logged on and unattended
- Attempt to gain administrative access to the School's network
- Engage in activities such as cracking passwords or maliciously accessing the Internet or other school social media accounts
- Attempt to disrupt use by other users, e.g. by deliberately wasting network resources, using other pupils workstation etc.
- Attempt to download compressed files (.arc .zip etc) without teacher permission.
- Attempt to play games online
- Attempt to listen to music online
- Attempt to download executable files
- Attempt to access proxy sites
- Post sensitive, defamatory or any information of inappropriate nature on school social media accounts that could bring the name of the school into disrepute or cause offence to other users of those accounts
- Attempt to do malicious damage to a workstation, or take action which might affect the operation of that workstation.
- Interfere with the computer of another pupil.
- Use any school social media accounts for a purpose for which it was not intended

The Internet and email

Students within school are given the opportunity to use the Internet, email and school social media accounts to further their studies in all the curriculum subjects. The use of the Internet, email and school social media accounts offers teachers and students many ways to enhance learning activities and provides access to materials that could not be otherwise used in the classroom.

As with all other school activities the use of ICT must be carefully planned and supervised. The school network keeps a log of all Internet activity and can identify which computer, and therefore which user, has visited any particular site at any given time. Users of school social media accounts also have their access monitored. In order to protect users from being accused of deliberately accessing inappropriate material the school has in place a procedure for reporting and recording such occurrences. This is in case of any downloading or viewing of inappropriate material, or using ICT inappropriately.

According to the LEA's acceptable use policy "Schools may wish to debate and define what they consider "inappropriate" for their individual communities but all would agree that explicit sexual, racist and violent materials would be unacceptable for viewing by staff and pupils."

As a school and a community we deem the use of the Internet, email and school social media accounts by a student for any other reason than to further their academic achievement as a misuse of the opportunity provided for them. Subsequently viewing or downloading any material approaching the above definitions the school "considers" inappropriate and is dealt with seriously.

Throughout the system pupils must **NOT**:

- Send emails anonymously or emails purporting to come from someone else
- Send messages via a school social media account purporting to come from someone else
- Send or display pornographic, offensive, defamatory messages or pictures
- Copy material from a website or message from a school media account and claim it is you
- Violate copyright laws. The downloading and/or distribution of music or video files for which license fees and distribution rights have not been paid or agreed upon constitutes an infringement of copyright, trademark and intellectual property rights and is illegal
- Store any material in your user area which is not directly required for schoolwork
- Use chat rooms **UNLESS** this forms part of a lesson supervised by a member of staff
- Harass, insult or attack others.

Prestwich Arts College uses third-party software to block websites which are illegal or which the school deem inappropriate. Inevitably, not all unsuitable sites will be blocked.

Pupils must not:

- Attempt to access inappropriate material such as pornographic, racist, or other offensive material.
- Attempt to go on sites such as YouTube, Twitter and Facebook including accessing at home, to post comments about existing and past members of staff or pupils. Defamatory comments will be challenged.

Moreover:

- The School accepts no liability in the unlikely event that damage (hardware, software or data) is sustained to a pupils' device as a result of its being connected to our network, with or without permission.

Prestwich Arts College takes incidents of the misuse or abuse of ICT (including cyber bullying) very seriously. All members of the school community have a clear role to play in reporting such incidents. Any student or parent concerned about an act of misuse of abuse should report the incident immediately to a member of staff. Students may also report instances anonymously through the Sharp system via the school website, or online at www.ceop.gov.uk, or via the local police.

Mobile Phones

The school's mobile phone policy has recently been updated and is followed meticulously. Therefore this section will not reiterate the information in that document but will discuss the issues that link mobile phones and ICT within the school.

In particular in school, mobile phones must not:

- Be used to record still or moving images or to record sound without the permission of a member of staff
- Be used to send offensive messages which harass, insult or attack others
- Be used to access websites that the school deems inappropriate
- Be used as calculators or watches in class
- Be used for social networking sites such as Facebook and Twitter
- Be used for accessing school social media accounts whilst in school

The following points are worth noting:

- Inappropriate material, accessed out of school, should not be brought into school and shared with others
- The School reserves the right to check the contents of all mobiles brought into school by pupils, and the right to remove material deemed inappropriate from such devices
- Pupils caught using their mobiles in a way deemed inappropriate will have their mobiles confiscated. They will be returned as outlined in the main mobile phone policy document.

'Blogs' and Social Networking: advide for use outside school

Some pupils at Prestwich Arts College have set up their own 'Blogs' – a sort of online diary which other people can access and read. Pupils also post messages and images to Social Networking sites such as Facebook. Obviously care must be taken about what is written on such sites particularly if mention is made of the School, its pupils and staff.

Access to these sites, from the School's internet service, has been and will continue to be blocked and as such their use is prohibited. Reading and writing to these sites should not be possible within the school. Parents should be aware of these sites and the possibilities of abuse. Software is available, free of charge, to block these sites and the content they have.

The school uses a number of social media accounts (which may use other software sites such as twitter as hosts). These sites will run only during school terms, and will not run during school holidays. They are for use by students when not in school. Any student using any of these accounts will adhere to the above policy, and any inappropriate behavior whilst using any of these sites will man the student being blocked form using that site in the future, and further school sanctions will also be considered.

Teaching and learning

The Computing scheme of work explores the main aspects of e-safety and is followed whenever students are using ICT. The issue of cyber bullying and personal safety is explored within the PHSE curriculum and the Tutorial Time programme and well as in other curriculular areas as appropriate. This also links with other work such as anti-bullying, respect, and relationships. It is acknowledged school council and the prefect group have a part to play in promoting this policy.

Digital recording devices (cameras, video cameras, ipads, etc) should only be used with staff supervision, and any instruction given by members of staff to students must be followed.

SIMs Learning Gateway

Information made available through PAC SLG is confidential and protected by law under the Data Protection Act 1998. To that aim you must not distribute or disclose any information obtained from the PAC SLG to any other persons with the exception of your parents. You should not attempt to access the PAC PLG in any environment where the security of the information contained in the PAC SLG may be placed at risks, for example in public places.

Passwords. You must assume personal responsibility for your username and password. Never use anyone else's username or password. You must always keep your username and password confidential, and must never be disclosed to anyone else. They should never be shared. You have the right to change your password, according to the following rules:

At least 6 characters, with at least one number, and not contain your own name or parts of your name.
You will be asked to change your password every 180 days.

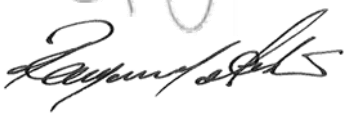
Prestwich Arts College reserves the right to revoke or deny access to PAC SLG of any student if you are found breach of this policy.

Prepared by: **Mr G T Newman Deputy Headteacher**

Date Reviewed: **November 2015**

Next Review Date : **November 2018**

Signed:  **Mr C C Hornby, Head Teacher**

Signed:  **Mr R Austin, Chair of Governors**

Protection of Children Act 1978 - take / make / distribute indecent photographs / pseudo photographs of children

NARRATIVE

Section 1 of the Protection of Children Act 1978 creates various offences regarding the taking, making or distributing indecent photographs (or pseudo-photographs) of a child.

1(1) Subject to sections 1A and 1B, it is an offence for a person -

(a) to take, or permit to be taken, or to make, any indecent photograph or pseudo-photograph of a child; or
(b) to distribute or show such indecent photographs or pseudo-photographs; or
(c) to have in his possession such indecent photographs or pseudo-photographs, with a view to their being distributed or shown by himself or others. or
(d) to publish or cause to be published any advertisement likely to be understood as conveying that the advertiser distributes or shows such indecent photographs or pseudo-photographs or intends to do so.

1(2) For the purposes of this Act, a person is to be regarded as distributing an indecent photograph or pseudo-photograph if he parts with possession of it to, or exposes or offers it for acquisition by, another person.

1(3) Proceedings for an offence under this Act shall not be instituted except by or with the consent of the Director of Public Prosecutions.

1(4) Where a person is charged with an offence under subsection (1)(b) or (c), it shall be a defence for him to prove -

(a) that he had a legitimate reason for distributing or showing the photographs or pseudo-photographs or (as the case may be) having them in his possession; or
(b) that he had not himself seen the photographs or pseudo-photographs and did not know, nor had any cause to suspect, them to be indecent.

1(5) References in the Children and Young Persons Act 1933 (except in sections 15 and 99) to the offences mentioned in Schedule 1 to that Act shall include an offence under subsection (1)(a) above.

1(6) *repealed*

1(7) *repealed*

Notes
(i)The term 'make' includes downloading images from the internet and storing or printing them out (R v Bowden (J) 1999). This concept was expanded in the later cases of R v Smith and R v Jayson 2002, which stated that deliberately opening an indecent computer email attachment or downloading an indecent image from the internet, so it can be viewed on a screen, is 'making' a photograph. The image does not have to be stored so it can be retrieved. Such an act must be done deliberately, innocently opening such a file is not an offence. For example, if

- *if an email attachment was opened innocently and not subsequently deleted due to a genuine lack of skill (deleting an email in 'Outlook' may only move it to a 'deleted ' directory, much like the 'recycle bin', this directory needs to be emptied and there may be other 'temporary' directories where it could be held);*
- *if an image was innocently downloaded from the web and immediately deleted without realising that the computer has stored a backup copy in a temporary internet directory,*

then no offence would be committed.
(ii) The words "shown by himself" means - shown by himself to other people. It is not an offence under this legislation to possess photographs to show to oneself, that is dealt with by section 160 of the Criminal Justice Act 1988. For implications on charging and sentencing see notes in R v Bowden.
(iii) Be aware of the powers of entry, search and seizure under the Act.
(iv) It is for a jury to decide the age of an unknown child seen in a photograph (R v Land 1997). It is important to realise that for sub-section 1(1)(c) of this offence the courts will ***NOT*** *accept an intent by the offender to show photographs to himself as sufficient to prove the offence (R v T 1999).*
(v) The above offences are included in Schedule 3 to the Sexual Offences Act 2003. Therefore a person convicted or cautioned for this offence must comply with the requirements of section 80 of that Act.
(vi) The above offences are also included in Schedule 2 to the Sexual Offences Act 2003. Therefore a person committing this offence outside the United Kingdom may in certain circumstances be prosecuted for that offence in England, Wales or Northern Ireland.
(vii) In a recent Crown Court case the "Trojan Horse" virus defence was successful. In short, expert evidence confirmed the likelihood of this virus being responsible for 14 depraved images saved on the defendant's personal computer. It was accepted that these could have been sent remotely, without the defendant's knowledge. Although the case is not binding on any other court, and each case will be determined according to its own particular facts, officers should be aware of the possibility should such a defence be raised.
(viii) The penalty applied on conviction will take into account the seriousness of the offence, which includes the category of the indecent image(s) and the number of images. The category can be determined by reference scale provided by the Sentencing Guidelines in respect of Offences Involving Child Pornography (see R v Oliver & others (2003) 1 Cr App R (S) 463 and R v Thompson (2004) Court of Appeal, Case No. 2004 00140 A4). The images should be catalogued on form MG6 and the information presented for each image on the schedule should include -

whether the image is a photograph or pseudo photograph;
the Category of the image
the age of the child (if not known estimated apparent age).

(ix) From 1st April 2014 the COPINE levels are replaced by Sexual Offences Definitive Guidelines from the Sentencing Council, the table and accompanying notes below have been taken from the guidelines (page 75 onwards for information relating to indecent images).

	Possession	***Distribution****	***Production*****
Category A	*Possession of images involving penetrative sexual activity* *Possession of images involving sexual activity with an animal or sadism*	*Sharing images involving penetrative sexual activity* *Sharing images involving sexual activity with an animal or sadism*	*Creating images involving penetrative sexual activity* *Creating images involving sexual activity with an animal or sadism*
Category B	*Possession of images involving non-penetrative sexual activity*	*Sharing of images involving non-penetrative sexual activity*	*Creating images involving non-penetrative sexual activity*
Category C	*Possession of other indecent images not falling within categories A or B*	*Sharing of other indecent images not falling within categories A or B*	*Creating other indecent images not falling within categories A or B*

** Distribution includes possession with a view to distributing or sharing images.*
*** Production includes the taking or making of any image at source, for instance the original image.*

Making an image by simple downloading should be treated as possession for the purposes of sentencing.

In most cases the intrinsic character of the most serious of the offending images will initially determine the appropriate category. If, however, the most serious images are unrepresentative of the offender's conduct a lower category may be appropriate. A lower category will not, however, be appropriate if the offender has produced or taken (for example photographed) images of a higher category.

MODE OF TRIAL AND PENALTY

Either Way
Summary: maximum 6 months imprisonment and / or a fine.
Indictment: maximum 10 years imprisonment.

Consent of the DPP required