Netherleigh and Rossefield School

Policy for Acceptable ICT usage (all staff)

January 2016

Access to computers/laptops and the Internet is a necessary tool for staff. It should be noted that the use of a computer system without permission or for a purpose not agreed by the school could constitute a criminal offence under the Computer Misuse Act 1990 and the Police and Justice Act 2006 (sections 35-38). Note that this policy applies to the use of all school equipment, whether in school or at home. Breaches of the Acceptable use Policy by staff will be reported to the Headmaster and will be dealt with according to the school's disciplinary policy or through prosecution by law.

All members of staff, students on placement, supply teachers etc must sign a copy of this policy statement before a system login password is granted.

Security

- Do not attempt to gain unauthorized access to information or facilities. The Computer Misuse Act 1990 makes it a criminal offence to obtain unauthorized access to any computer (including workstations and PCs) or to modify its contents. If you don't have access to information resources you feel you need, contact the ICT teacher.
- Do not disclose personal or system passwords or other security details to children or volunteers. If a child gets to know your password, ensure you change it or inform the ICT Coordinator, who will ensure the password is changed.
- If you leave your PC/laptop unattended without logging off, you are responsible for any misuse of it while you're away.

Failure to keep passwords safe can compromise network security.

Anti-virus

The integrity of the school's computer systems is put at risk if users do not take adequate precautions against malicious software, such as computer viruses. All staff must ensure that any computer, for which they have responsibility, is adequately protected against viruses, through the use of up to date anti-virus software.

Staff should also be aware that memory sticks are a common means of attack for computer viruses and ensure that any memory sticks they are responsible for are regularly scanned for viruses.

If you do encounter a problem with viruses, you should immediately switch off the PC/laptop in order to stop the virus spreading, and report it to the ICT teacher.

Inappropriate Material

Inappropriate material: Don't write it, publish it, look for it, bookmark it, access it or download it. If you do happen across anything unsuitable, you must inform the appropriate authority as soon as you practically can. If this happens in school, inform the ICT teacher (or the Headmaster/Deputy Head, or other member of the management team, if the ICT teacher is unavailable), who will ensure the website is blocked and will record what has happened, and the action taken. Staff should be aware that any access of inappropriate material could lead to disciplinary and/or legal action.

Data Storage

Keep copies of important data on the network and not solely on your PC/laptop or memory stick. Otherwise it will not be backed up and is therefore at risk.

Children and the Internet.

All children must understand that if they see an unacceptable image on a computer screen, they must turn the screen off and report immediately to a member of staff. Children must not be given unsupervised access to the Internet. For the purposes of this policy, “supervised” means that the user is within direct sight of a responsible adult.

Equipment Issues.

Occasionally, equipment and/or software may not work – such is the nature of ICT equipment. Staff should inform the ICT teacher who will fix it where possible, or inform our ICT support.

Copyright

Copyright of materials must be respected. When using downloaded materials, including free materials, the Intellectual Property rights of the originator must be respected and credited.

Publication on the School Website.

No video recording may be published without the written consent of the parents/legal guardian of the child concerned, and the child’s own verbal consent.

Surnames of children should not be published, especially in conjunction with photographic or video material;

No link should be made between an individual and any home address (including simply street names);

Where the person publishing material suspects that there may be child protection issues at stake, then serious consideration must be taken as to whether that material may be published or not. In the case of a simple piece of art work or writing, it may well be fine, but images of that child should not be published. If in any doubt at all, refer to the person responsible for child protection.

Social Networking Sites

- To ensure that your Facebook account does not compromise your professional position, please ensure that your privacy settings are set correctly.
- Do not under any circumstances accept friend requests from a person you believe to be either a parent or a pupil at your school, or use social media to communicate with anyone you believe to be a parent or pupil.

As a minimum, we recommend the following:

Privacy Setting	Recommended security level
Send you messages	Friends only
See your friend list	Friends only
See your education and work	Friends only
See your current city and hometown	Friends only
See your likes, activities and other connections	Friends only
Your status, photos, and posts	Friends only
Bio and favourite quotations	Friends only
Family and relationships	Friends only
Photos and videos you're tagged in	Friends only
Religious and political views	Friends only
Birthday	Friends only
Permission to comment on your posts	Friends only
Places you check in to	Friends only
Contact information	Friends only

- Always make sure that you log out of Facebook after using it, particularly when using a shared machine. Your account can be hijacked by others if you remain logged in – even if you quit your browser and/or switch the machine off. Similarly, Facebook's instant chat facility caches conversations that can be viewed later on. Make sure you clear your chat history on Facebook (click "Clear Chat history" in the chat window).
- Employers may scour websites looking for information before a job interview. Take care to remove any content you would not want them to see.

- Do not make disparaging remarks about your employer/colleagues. Doing this will be deemed as bullying and/or harassment, as it would be if done in person, and will lead to disciplinary action.
- Act in accordance with this policy.
- Other users could post a photo on their profile in which you are named, so think about any photos you appear in. On Facebook, you can 'untag' yourself from a photo. If you do find inappropriate references to you and/or images of you posted by a 'friend' online, you should contact them and the site to have the material removed.
- Parents and students may access your profile and could, if they find the information and/or images it contains offensive, complain to your employer.

- If you have any concerns about information on your social networking site or if you are the victim of cyberbullying, you should contact your line manager immediately.
- Do not publish your date of birth and home address on Facebook. Identity theft is a crime on the rise with criminals using such information to access to your bank or credit card account.
- Stop the network provider from passing on your details to other companies for research and advertising purposes. For example, to stop Facebook from forwarding your details, click “Privacy Settings”. Under “Applications and websites” click “edit your settings”. Scroll down to “instant personalisation” and make sure the checkbox for “enable instant personalisation on partner websites” is unchecked.
- Ensure that any comments and/or images could not be deemed defamatory or in breach of copyright legislation.

While the guidance above focuses on Facebook, the same advice applies to Twitter, Instagram and any other social networking/social media site. Similarly, references to pupils should be understood to include former pupils.

It is a condition of your employment that you agree to abide by this policy.

Failure to abide by this policy may lead to disciplinary action, and, where appropriate, legal action, including referral to the police.

Signed……..

Date ……..

(School Office retains a list of staff signatures which confirms employee willingness to comply with the above policy.)