FLYING BULL PRIMARY AND NURSERY SCHOOL

Use of School Computer Network

Introduction

The Computer Network is provided for the use of pupils and staff at the Flying Bull Primary and Nursery School to support and enhance the delivery of the curriculum. Every teacher and support staff employee who needs it is allocated their own log-in ID, password and network disk space.

Status of the Guidelines

These guidelines do not form part of the formal contract of employment for staff. However it is a condition of employment that users will abide by the rules and policies of the School. Any failure to follow the guidelines can therefore result in disciplinary proceedings. If the contravention is deemed illegal, formal legal proceedings may be taken.

Conditions of Use

Staff should be aware of the main pieces of UK legislation which apply directly to computing systems in School.

The Computer Misuse Act 1990

In essence this Act makes it an offence to access, or try to access, any computer system for which access authorisation has not been given. Thus any attempt to interfere with, or try to bypass, the security controls on a computing system is an offence. Similarly, trying to obtain information, such as other users' passwords, or accessing or modifying files belonging to other people who have not given access authorisation is also an offence. Further information on the Act is available from the government printing office at http://www.opsi.gov.uk/acts/acts1990/UKpga_19900018_en_1.htm.

The Copyright, Designs and Patents Act 1988

This Act makes it an offence to copy material, either paper-based or electronically stored without the permission of the owner of the copyright. It applies to all software in use in the School as well as text, images and programs on the Internet. Further information on the role of the Copyright Licensing Agency may be found at http://www.cla.co.uk/.

Further information on the Act is available from the government printing office at:
http://www.opsi.gov.uk/acts/acts1988/UKpga_19880048_en_1.htm.

Data Protection Act 1984 (new Act 1998)

In summary the eight main principles are that all personal data shall be:

(1) obtained and processed fairly and lawfully

(2) held only for lawful purposes which are described in the register entry

(3) used or disclosed only for those or compatible purposes

(4) adequate, relevant and not excessive in relation to the purpose for which they are held

(5) accurate and, where necessary, kept up-to-date

(6) held no longer than is necessary for the purpose for which they are held

(7) able to allow individuals to access information held about them and where appropriate correct or erase it

(8) surrounded by proper security

Further information on the Act is available from the government printing office at :
http://www.opsi.gov.uk/Acts/Acts1998/ukpga_19980029_en_1

Computers and the Local Area Network

Staff have access to more information on the network than do pupils, so it is essential that staff should never:

• divulge their password to a pupil

• allow a pupil to use a computer unsupervised if it has been logged in under a staff ID

• leave a computer logged in and unattended in vulnerable areas without locking the room

If you have any reasons to suspect that others know your password then change it at once. Any damage or changes made under your ID will be your responsibility.

Staff should contact IT Support before attempting to permanently change the configuration of any computer. No user should copy software from or to any school computer or network in violation of our licensing agreements.

Staff should be aware of the Health and Safety issues of using IT equipment. In particular, any use for extended periods should be broken by regular breaks to avoid repetitive strain injury and eye strain.

Computer viruses and other damaging software can be very expensive and time wasting in their effects. Please use virus checking software provided on the network to check any disks or memory sticks you have brought in from home or data you have downloaded from outside the school.

At no time may the school computing or telecommunications facilities be used for the storage, display or transmission of material, in any format, that is abusive, racist, pornographic, or terrorist in nature. The school reserves the right to monitor any data stored on its equipment or transmitted to or from its site. Users, without permission of the ICT Leader, should not attempt to password-protect or encrypt any data as it may be assumed to be suspect.

The school takes no responsibility for data stored on the network or data lost due to computer failure. We do, however, take every precaution to maintain network data integrity including taking nightly back-ups. Disk space is limited and, while we try to accommodate all users' needs in this respect, sensible restrictions have to apply. Old files that have not been accessed for a long time may be archived to tape storage to free up disk space.

The quantity of IT equipment in the school is limited. For this reason priority must always be given for school-related work during the normal working day.

Internet

Most of the School computers are set up to allow access to the Internet. The Internet can be a valuable tool for research and communication, but it can also be a time and resources waster and does have some risks. Please follow these guidelines within the School:

• Our connection to the Internet is via Portsmouth IT Services. We have to conform to their Acceptable Use Policy which is available from PCC.

• Internet access during the school day is for school-related work only.

• Copying text or images from the Internet may breach the Copyright, Design and Patent Act. Please check with the owner before copying or publishing such material.

•The school Internet access is filtered to block undesirable sites. If you need access for a valid reason to a blocked site please contact IT Support.

•Staff may develop pages for the school website. These pages should not be used for any purpose that would detract from, or be detrimental to, the reputation of the school.

• If you use e-mail please refer to the separate conditions of use document.

Social networks (including Facebook)

This guidance is provided to outline expectations of staff at Flying Bull Primary and Nursery in relation to communication between staff and pupils. The policy is the result of our responsibility to safeguard the health, safety and emotional well-being of the children in our charge is met. In addition, we must ensure that we are able to safeguard our own and others professional reputations against the possibility of malicious allegations.

As the use of Internet chat rooms and social networks develop it is vital that school staff are only engaged in communicating with pupils through:

Professional, moderated ways of communicating with our pupils:

- In lessons
- In formal meetings
- In clubs, visits out of school hours where the parents have been informed of the purpose and content in advance

The school website may contain messages and information for specific educational purposes. These are moderated by staff.

Sites included on the Flying Bull Primary approved website list.

Members of staff at Flying Bull Primary must NOT use the following methods of communication with pupils:

- Telephoning their mobile phones
- Instant message services such as MSN Messenger and Skype
- Having pupils as friends on social networking sites such as FaceBook
- Blogging, Wiki, Twitter or Web 2.0 sites unless they are part of the Flying Bull Primary approved list

Teachers' official blogs or wikis should be password protected and run from the school website. Teachers are advised not to run social network spaces for student use on a personal basis and MUST NOT communicate through such sites, passive or otherwise.

All members of staff must be mindful of the fact that messages, posts, tweets, status updates, etc made on electronic media are capable of being read by the public at large. This can be directly (e.g. Twitter) or indirectly (e.g. Facebook),

regardless of privacy settings. Comments that may be interpreted as bringing the organisation (i.e. Flying Bull Primary or Portsmouth City Council) into disrepute are disciplinary matters.

You are strongly advised not to find yourself in this position. You are strongly recommended not to use these media to make comments about your work, employer, colleagues, pupils or their families, either individually or generally.

Feedback to colleagues or issues you wish addressing should be raised in the first instance with your phase leader, member or a member of the senior leadership team, not through publically available electronic media.

It is essential that staff that have accepted current pupils as friends or contacts on MSN, Facebook or any other social networking site to delete them with immediate effect.

Printing

Print credits are in place to remind employees to print with care. They are not intended to restrict necessary printing.

Computer Use at Home

Any processing of school personal information is covered by the Data Protection Act and the user at home should take similar safeguards to protect the information from unauthorised access.

Use of USB memory sticks (including all forms of flash and hard drive memory devices e.g. MP3 players)

Sensitive pupil's data (SEN, contact details, etc) should not be stored on unsecure memory devices. Due to the risks of losing memory sticks it is recommended that sensitive data remains on the school network or e-mailed using the school e-mail account. The use of sensitive data on staff computers, both personal and school issued, should be minimised and login passwords should be used at all times. Encryption software is available without cost from http://www.rohos.com/products/rohos-mini-drive/ or http://www.truecrypt.org/ to secure staff memory sticks and computers.

N.B. Where possible, use remote access.

Intellectual Property Rights

The school ICT Policy states that the school may claim the intellectual copyright on any material produced on its ICT equipment by an employee. If any member of staff is in any doubt about the intellectual property rights on any materials they are working on they should first check with the Local Authority.

Archived Media (Backing Storage e.g. Floppy Disks, CD-R/RW, Backup drives)

Data stored on archive media must be kept in a secure location. Historic data may still be sensitive and it is imperative members of staff who have backups of such data keep it in a safe location either at home or in school.

Written: 9.11.2011