ICT Acceptable Usage Policy

Policy/Procedure Title	ICT Acceptable Usage Policy
Author	*OCC Model adopted annually and updated in line with OCC updates*
Approved by	*PAT Directors*
Reviewed	*Jan 2020*
Review date	*Jan 2021*

Scope

This policy applies to all users of ICT systems within the Propeller Academy Trust (PAT). Any reference to "school" applies to Kingfisher School and Fitzwaryn School and to employees, temporary staff and volunteers whether at work, home or elsewhere.

Policy

Employees who breach any of the terms in this policy, deliberately or through negligence may be subject to disciplinary action.

Introduction

Every user is responsible for the proper use of his/her equipment.

School equipment should not be used in any way for salacious, illegal, libellous or defamatory material or purposes that could bring the PAT and therefore the school into disrepute.

User Responsibilities

As a user of PAT ICT facilities you are responsible for:

- Informing your manager if you believe that others are using systems inappropriately.
- Notifying the ICT Technician if you think that someone else may be using your login details
- Safeguarding personal/confidential data
- Contacting the ICT Technician immediately in the event of a suspected virus infection
- Ensuring that personal use of ICT equipment remains very occasional and reasonable and does not interfere with everyday workload and commitments or endanger either School's systems.

Managers' responsibilities

Managers are responsible for ensuring that all their employees are aware of this policy and act in accordance with its requirements.

Privacy

All systems may be monitored and audited for administrative and maintenance purposes so personal privacy cannot be assumed.

Systems may be accessed at management discretion during an individual's absence where essential to the running of the school.

Security & Integrity of Systems & Equipment

All use of School ICT equipment is subject to authorisation. As a user, you will be issued with one or more user IDs and associated passwords to enable authorised use. Your user

ID is intended for your use alone. You must not permit its use by others except when required to do so in order to facilitate critical operations.

- Do look after your passwords

- Do not remove security measures on any system. Logout or lock your computer if you leave your workstation unattended. You are responsible for any misuse of systems or data accomplished with your login information.

- You must not use ICT facilities to access, transmit or share material that is confidential to the PAT, or is confidential to an individual, without the appropriate permission.

Bear in mind the following:

- Do obtain authorisation from the ICT Technician for the installation of additional software on any equipment

- Do not change the configuration of installed ICT equipment unless authorised to do so.

- Do not access or attempt to access any ICT system for which you are not an authorised user.

- Do not connect non-school equipment to either school network unless authorised to do so.

- Do not remove school-based ICT equipment or software without authorisation.

- Do not let friends or family use school equipment assigned to you.

- Do make sure that all critical documents are held on a network drive rather than the PCs/laptop's hard drive (if this is impractical then ensure these documents are regularly copied to a back-up medium so as to minimise the loss in case of equipment failure. If they are backed up onto memory sticks/CDs then they must be kept secure).

- Unless there is a legitimate need, do not connect any digital media devices or load their associated software

Use of e-mail

Users must not e-mail confidential information outside of the school email system.

Comply with the e-mail and internet usage policy

Working at home/remote working using school equipment or personal equipment

This policy applies to employees when working from school, home or other location. Work carried out must always be with due regard to the terms of this policy and to data protection/ confidentiality issues.

Confidential data and documents must not be stored long term on non- School equipment.

Very sensitive documents additionally should be password protected or otherwise encrypted to prevent unauthorised access.

Always ensure that at least one other person knows the password to retrieve information that you have encrypted.

Use of the Internet

Guidelines for acceptable use:

- Never attempt to access illicit or inappropriate web sites. Inform your manager straight away if you accidentally access an illicit/inappropriate website.

- Respect the laws protecting copyright and intellectual property rights. Downloading and storage of copyright material like music and video files may be illegal. Where such files are found on ICT equipment without a bona fide reason, files will be deleted.

- School's ICT equipment and services should not be used for personal business activity, fundraising or advertising.

- Access of non-work related websites is permitted only in your own time.

- Accessing personal web-mail sites in the user's own time is acceptable provided personal e-mails are not stored on School systems and equipment.

- Use of peer-to-peer file sharing technologies is strictly forbidden.

- Instant messaging is not permitted other than using School-supplied systems.

- Selling or taking part in online auctions etc is not permitted.

- On-line gambling is not permitted.

Monitoring

Information about network traffic may be logged in connection with:

- Automated filtering of inappropriate incoming/outgoing e-mails
- Routine administrative/maintenance purposes
- Compliance with School policies

All equipment provided by School may be monitored and audited for administrative and maintenance purposes.

Any external storage device attached to School equipment may also be monitored and audited. By connecting a device to School equipment, you consent to its monitoring and auditing during the time it is connected.

Misuse of ICT equipment or systems

Where users make inappropriate or excessive personal use of systems or there is persistent or serious misuse, disciplinary action may result. Where

equipment or systems are used to access or engage in illegal activity, the police will be informed and disciplinary action will also be taken.

This Policy should be read in conjunction with the Use of Videos and Photographs Policy and Staff Code of Conduct particularly with reference to the use of social media eg facebook.