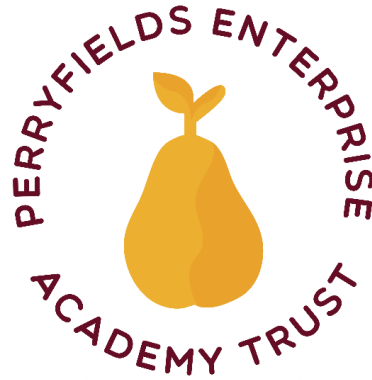


Perryfields Enterprise Academy Trust

Acceptable Use Policy



Perryfields Enterprise Academy Trust	
Adapted From:	ECC H.R Policy
Approved By:	P.E.A.T Board
Approved Date:	26 May 2017
Review:	Every 3 years
Next Review Date:	May 2020 or as advised by H.R. Provider – EEC
Signed by Executive Chair:	
Published on	PEAT website

Perryfields Enterprise Academy Trust

Acceptable Use Policy

Aims and Responsibilities

This policy applies to ALL users regardless of their position in P.E.A.T.

The Aim

To develop an environment where ICT underpins teaching, learning, management and administration across the Academy

PEAT schools subscribe to a number of curriculum-based software packages. SIMs management is used in school offices and is on a separate system to the rest of the school.

Training is made available at regular intervals to ensure that staff can update their ICT knowledge and learn new skills to enable them to fulfil the expectations of their role.

Responsibilities

All users are expected to act responsibly and to show consideration to others. Staff are expected to guide pupils in appropriate ways of engaging with on-line facilities that will support the learning outcomes appropriate to their age and ability. Students should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

All staff have a responsibility to teach what is acceptable and what is not acceptable when using on-line resources and to take appropriate action if they are aware of occasions when student use does not follow the Acceptable Use Policy.

Equipment Security

- Teaching staff are allocated a laptop which may be used from home. Staff should ensure that they do not leave their laptop in their car and that their home insurance covers its loss.
- Staff have a responsibility to ensure that moveable equipment such as laptops and remote control units are securely stored during and at the end of the day.

Security

- Staff are responsible for the protection of their own network and SIMs login accounts and should not divulge passwords to anyone. Joint passwords for sites should also be carefully protected.
- No pupil is allowed to use a computer allocated to a member of staff without prior permission.
- Users should not log on as someone else, nor use a computer which has been logged on by someone else.
- Users should change their passwords regularly
- Users should also log off or lock the keyboard (using CTRL+ALT+DEL) when leaving a workstation, even for a short time.

- Access to the Internet is filtered to prevent access to inappropriate sites, and to protect the computer systems. Users should be aware that the school logs all Internet use for all users.
- Users should ensure that they are not breaking copyright restrictions when copying and using material from the internet.
- Legally, children are not allowed to take and store photographs of staff or other children without their written permission (in accordance with the Data Protection Act 1998)
- Users should be aware that the school has a right to access personal folders on the network. Privacy will be respected unless there is reason to think that the ICT Acceptable Use Policy or school guidelines are not being followed.

Remote Access

This policy applies to remote access users where applicable with the following additions:

- Users must ensure that they log off when they have finished.
- Only Staff members are permitted to access school equipment and management software.
- Users should be aware that remote access is logged and can be monitored.
- Some information held on the school network may be confidential and therefore must be treated with due care and consideration.

Use of other technology

- Pupils are not permitted to have technology such as media rich phones and MP3 players in school. Staff are expected to support this policy and take appropriate action if necessary
- Personal Digital Assistants (PDA), memory cards, USB Storage Keys and anything else that can be used to store, transmit or manipulate data should be used responsibly, and in accordance with ICT Acceptable Use Policy. Students using such devices must not be connected to the school network without specific permission.

Use of the school network and other related facilities

It is **not acceptable** to:

- Attempt to download or install any programs to a school owned computer.
- Attempt to introduce a virus, or malicious code.
- Attempt to bypass network and systems security.
- Attempt to access another user's account.
- Attempt to gain access to an unauthorised area or system.
- Attempt to use any form of hacking or cracking software / system.
- Access, download, create, store or transmit material which is indecent or obscene, or material which could cause annoyance, offence or anxiety to other users, or material which infringes copyright, or material which is unlawful.
- Wilfully damage or tamper with any network equipment

Staff need to be aware that all networked computers in the school are monitored remotely. Emails are automatically monitored via the e-folio filter.

Personal laptops/ Computers and Staff Laptops

- Personal laptops and computers can be connected to the school network only after consulting the ICT department. They are subject to the ICT Acceptable Use Policy, and in addition, all computers must be subject to a Technician check before being connected to the network.
- All computers must use the computer naming convention configured by the school.
- All computers should, for their own protection, have the school managed Anti-Virus software installed.
- In the case of Staff laptops, no other software other than the approved school software should be installed without consultation with the ICT technicians.

Use of the Internet

DISCLAIMER

No warranties of any kind whether expressed or implied are made for the network service provided.

No responsibility can be accepted for any damages suffered whilst on this system. These damages include loss of data as a result of delays, non-deliveries, miss-deliveries or service interruptions caused by the system or elements of the system, or your errors or omissions. Use of any information obtained via the network or other information systems is at your own risk.

Perryfields Enterprise Academy Trust denies any responsibility for the accuracy of information obtained via its Internet services.

Disciplinary Procedures

Those who misuse the computer facilities and contravene the ICT Acceptable Use Policy will be subject to disciplinary procedures.

Monitoring and review

This policy is monitored by P.E.A.T LGBs, and will be reviewed in three years, or earlier if necessary.