THINKING SCHOOL ACADEMY TRUST

The Portsmouth Academy

e-Safety Policy

‘Aspire and Achieve’

Lead Professionals:	Assistant Principal: Every Child Achieves Designated Safeguarding Lead (DSL)
Agreed:	December 2016
Planned Review Period:	Annually
Planned Review Date:	December 2017
Governor Committee:	Behaviour & Wellbeing

The Portsmouth Academy e-Safety policy

The e-Safety Policy relates to other policies including those for e-Learning, Social Media, Anti-bullying, Safeguarding, Acceptable use, and the Code of Professional Values and Practice.

The school has a nominated e-Safety coordinator. At TPA this is the Designated Safeguarding Lead.

Teaching and learning

Why the Internet and digital communications are important

At TPA we believe that the Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with high-quality Internet access as part of their learning experience.

Internet use is a part of the statutory curriculum and a necessary learning tool for staff and pupils.

Internet use will enhance and extend learning

The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.

Clear boundaries will be set for the appropriate use of the Internet and digital communications and discussed with staff and pupils.

Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

Pupils will be taught how to evaluate Internet content

TPA will ensure that the use of Internet derived materials by staff and by pupils complies with copyright law.

Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Managing Internet Access

Information system security

The TPA ICT system security is reviewed regularly.

Virus protection is installed and updated regularly.

Security strategies are discussed with the Local Authority.

E-mail

PUPILS:

Pupils may only use approved e-mail accounts on the school system.

Pupils must immediately tell a member of staff if they receive offensive e-mail.

In e-mail communication, pupils must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.

Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.

The school should consider how e-mail from pupils to external bodies is presented and controlled.

The forwarding of chain letters is not permitted.

STAFF:

Staff email accounts may have fewer restrictions than pupil accounts to allow them more functionality for teaching purposes but will still be encompassed by the acceptable use policy.

Published content and the school web site

Staff or pupil personal contact information will not generally be published. The contact details given online e.g. on the school website, should be the school office. However, individual staff members may use their school email address for educational business, inside or outside of school.

The e-Learning Manager will take overall editorial responsibility and ensure that published content is accurate and appropriate.

Publishing pupils' images and work

Photographs that include pupils will be selected carefully so that individual pupils cannot be identified or their image misused.

Pupils' full names will not be used anywhere on a school Web site or other on-line space, particularly in association with photographs.

Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site. Work is only published with the permission of the pupil and parents/carers via a generic permission slip.

Social networking and personal publishing (See Social Media Policy)

The school will not allow pupils access to social networking sites, however it recognises its responsibility to educate pupils in their safe use.

Chatrooms will be blocked unless a specific use is approved.

Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location.

Pupils will be advised not to place personal photos on any social network space without considering how the photo could be used now or in the future.

Pupils will be advised on security and encouraged to set passwords, to deny access to unknown individuals and to block unwanted communications. Pupils should only invite known friends and deny access to others.

Managing filtering

The school will work in partnership with Portsmouth L.A. and the Internet Service Provider to ensure that systems to protect pupils are reviewed and improved.

If staff or pupils discover an unsuitable site, it must be reported to the e-Learning / Network Manager.

Senior leaders will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Managing emerging technologies

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

The senior leadership team should note that technologies such as mobile phones with wireless Internet access can bypass school filtering systems and present a new route to undesirable material and communications.

Mobile phones will not be used during lessons or formal school time without staff permission. The sending of abusive or inappropriate text messages and the taking of photographs without staff permission is strictly forbidden and may lead to disciplinary action.

The use by pupils of cameras in mobile phones for learning opportunities will be kept under review.

Games machines including the Sony PlayStation, Microsoft Xbox and others have Internet access which may not include filtering. Care is required in any use in school or other officially sanctioned location.

Staff will be issued with a school phone where contact with pupils is required.

Protecting personal data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

Policy Decisions

Authorising Internet access

All staff must read and sign the 'e-Learning Acceptable Use Agreement (Staff)' before using any school ICT resource.

The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.

Pupils must apply for Internet access individually by agreeing to comply with the e-Learning Acceptable Use Agreement (Pupil).

Parents/carers will be asked to sign and return a consent form.

Assessing risks

The school and the L.A will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school network. Neither the school nor the L.A. can accept liability for any material accessed, or any consequences of Internet access.

The school will audit ICT use to establish if the e-Safety policy is adequate and that the implementation of the e-safety policy is appropriate and effective using BECTA guidelines.

Handling e-safety complaints

Complaints of Internet misuse will be dealt with by a senior member of staff.

Any complaint about staff misuse must be referred to the Principal.

Complaints of a child protection nature must be referred to the DSL.

Pupils and parents are informed of the complaints procedure via the school prospectus.

Discussions will be held with the school's PCSO to establish procedures for handling potentially illegal issues.

Community use of the Internet

The school will liaise with local organisations to establish a common approach to e-Safety.

Communicating e-Safety

Introducing the e-Safety policy to pupils

e-Safety rules will be posted in all rooms where computers are used.

Pupils will be informed that network and Internet use will be monitored.

A programme of training in e-Safety will be developed, and delivered both to pupils and through Family Learning events.

Staff and the e-Safety policy

All staff will be given the School e-Safety Policy and its importance explained.

Staff will be informed that network and Internet traffic can be monitored and traced to the individual user.

Staff that manage filtering systems or monitor ICT use will be supervised by senior management and work to clear procedures for reporting issues.

Staff should understand that phone or online communications with pupils can occasionally lead to misunderstandings or even malicious accusations and must keep a record of any such contacts. Staff must take care always to maintain a professional relationship.

Enlisting parents' and carers' support

Parents' and carers' attention will be drawn to the School e-Safety Policy in newsletters, the school brochure and on the school Web site.

All parents will be offered e-Safety training through Family Learning sessions