Waterloo Primary Academy

E-Safety Policy

Approved: March 2017
Responsible Personnel: ICT Manager
Review Period: Annual
Review Date: April 2023

Zest Academy Trust

Writing and Reviewing the E-safety Policy

The E-Safety Policy is part of the Academy Development Plan and relates to other policies including those for ICT, bullying and for child protection. The academy's ICT Education Officer will also act as E-Safety Coordinator.

Our E-Safety Policy has been written by the academy, building on the government and CEOP E-Safety guidelines. It has been agreed by senior management and approved by governors. The E-Safety Policy and its implementation will be reviewed annually.

Teaching and Learning

Why internet use is important

The Internet is an essential element in 21st century life for education, business and social interaction. The academy has a duty to provide children with quality Internet access as part of their learning experience. Internet use is a part of the daily life, the curriculum and a necessary tool for staff and pupils.

Internet use will enhance learning

The Academy Internet access is designed expressly for pupil and staff use and includes filtering appropriate to the age of pupils. Pupils will be taught what internet use is acceptable and what is not and given clear objectives for internet use. 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

The Academy will ensure that the use of internet derived materials by staff and pupils complies with copyright law. Pupils should 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

Academy Network systems capacity and security will be reviewed regularly. Virus protection is updated regularly. Content filtering services will be updated from centrally recognised databases, conforming to current standards and requirements

Email

Pupils will be assigned email accounts. Pupils may only use approved e-mail accounts on the Academy system and email usage should be supervised and monitored by a staff member.

Pupils must immediately tell a teacher if they receive offensive e-mail.

Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.

E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on Academy headed paper.

The forwarding of chain letters is not permitted.

Published content and the Academy website

The Academy will be responsible for ensuring any published items meet requirements and do not infringe copyright. The website will contain information relating to the Academy and any works should be published on class blogs using our approved blogging tool – Google Blogger.

Publishing pupil's images and work

In the modern changing world, the academy wants to create an audience for the children and so will utilise multi-media appropriate web sites such as Picasso, YouTube Blogger etc. The Academy will publish video, photographic and audio recordings of the children. Pupils' full names will not be associated with any of the recordings. Parents and guardians will be given the opportunity to opt out and not have their child's recordings published.

Social networking and personal publishing

The Academy will monitor and block access to social networking sites.

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

Pupils and parents will be advised that the use of social network spaces e.g. Facebook, outside academy is inappropriate for pupils aged 12 or under.

Managing filtering

The Academy will work with the DfE, CEOP and make use of the academy's web filtering system to ensure systems to protect pupils are reviewed and improved.

If staff or pupils discover an unsuitable site, it must be reported to the E-Safety Coordinator.

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

Managing videoconferencing

Currently the unsupervised use of video conferencing including FaceTime is not permitted at any time. Videoconferencing will be appropriately supervised for the pupils' age

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students / pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents and students need to be aware of the risks

associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

When using digital images, staff should inform and educate students about:

- The risks associated with the taking, use, sharing, publication and distribution of images. In particular, they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.

- In accordance with guidance from the Information Commissioner's Office, Parents are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on
social networking sites, nor should parents comment on any activities involving other students in the digital / video images.

- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.

- Care should be taken when taking digital / video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.

- Students must not take, use, share, publish or distribute images of others without their permission, photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images. Students' full names will not be used anywhere on a website or blog, particularly in association with photographs. Written permission from parents or carers will be obtained before photographs of students are published on the school website Student's work can only be published with the permission of the student / pupil and parents or carers.

Managing emerging technologies

Emerging technologies will be examined for educational benefit and implemented where appropriate.

Mobile phones will not be used during lessons or formal academy time. The sending of abusive or inappropriate text messages is forbidden.

Protecting personal data

Data Protection

Personal data will be recorded, processed, transferred and made available according to the

Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

The school must ensure that:

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing".
- It has a Data Protection Policy
- It is registered as a Data Controller for the purposes of the Data Protection
- Act (DPA)
- Responsible persons are appointed / identified - Senior Information Risk Officer(SIRO) and Information Asset Owners (IAOs)
- Risk assessments are carried out
- It has clear and understood arrangements for the security, storage and transfer of personal data

- Data subjects have rights of access and there are clear procedures for this to be obtained. There are clear and understood policies and routines for the deletion and disposal of data. There is a policy for reporting, logging, managing and recovering from information risk incidents. There are clear Data Protection clauses in all contracts where personal data may be passed to third parties
- There are clear policies about the use of cloud storage / cloud computing
- which ensure that such data storage meets the requirements laid down by the **Information Commissioner's Office.**

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and Other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- When personal data is stored on any portable computer system, memory
- stick or any other removable media.
- the device must be password protected.
- the device must offer approved virus and malware checking software.
- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

Social Media – Protecting Professional Identity

All schools, academies and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place. The school provides the following measures to ensure reasonable steps are in place to minimise the risk of harm to pupils, staff and the school through limiting access to personal information:

- Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

School staff should ensure that:

- No reference should be made in social media to students / pupils, parents /

carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

The school's use of social media for professional purposes will be checked regularly by the senior risk officer and e-safety committee to ensure compliance with the Social Media, Data Protection, Communications, Digital Image and Video Policies

Policy Decisions

Assessing risks

The Academy will take all reasonable precautions to ensure that users access only appropriate 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 an academy computer or device. The Academy cannot accept liability for the material accessed, or any consequences of Internet access.

The Academy will audit ICT provision to establish if the e-safety policy is adequate and that its implementation is effective.

Handing e-safety complaints

Complaints of Internet misuse will be dealt with by the ICT Manager.

Any complaint about staff misuse must be referred to the ICT Manager.

Complaints of a child protection nature must be dealt with in accordance with academy child protection procedures.

Pupils and parents will be informed of the complaints procedure.

Communications Policy

Introducing the e-safety policy to pupils

E-safety rules will be on the academy's website and through the portal. E-safety will be discussed with pupils as the first ICT lesson of each half term and as part of our PSHE curriculum.

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

Staff and the e-safety policy

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

Staff should be aware that Internet traffic can be monitored and is not only traceable to the individual user, but also the location. Discretion and professional conduct is essential.

Enlisting parents' support

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

Internet Safety

All e-safety complaints and incidents will be recorded by academy – including any actions taken.

- Pupils and parents will be informed of the complaints procedure
- Parents and pupils will work in partnership with staff to resolve issues
- Academy will work with third parties to establish procedures for handling illegal issues

Incident Reporting

Details of all E-Safety incidents are to be recorded on the following form and then forwarded to the ICT Manager. The incident logs with be monitored termly by the Academy ICT Manager and then a report will be forwarded to the SMT.

E-Safety Incident Report

Date & Time	**Name of pupil or staff member**	**Computer Name / Device No**
Details of Incident		
Actions Taken		
Name		
Signature	**Date**	

Think! - Then Click.

Think! - Then Click
e-Safety Rules for the Academy
• We only use the Internet with permission. • We tell an adult if we see anything we are uncomfortable with. • We close any webpage we are not sure about. • We only send e-mails that are polite and friendly. • We never give out personal information or passwords. • We never arrange to meet anyone we don't know. • If we receive unkind messages or emails, we don't delete them but tell an adult straight away.

Appendix A

Both in school and at home, children are able to access the internet in a variety of ways: home computers, IPADs, laptops, smartphones and games consoles. When your child accesses the internet, it is important that they are monitored closely.

Simple rules for keeping your child safe

- Ask permission before using the Internet and discuss what websites they are using
- Only use websites you have chosen together or a child friendly search engine (www.askkids.com, www.kids.yahoo.com, www.bbc.co.uk/cbbc/search, www.kidsclick.org)
- Only email people they know (why not set up an address book?)
- Ask permission before opening an email sent by someone they don't know
- Not use their real name when using games or websites on the internet (create a nickname)
- Never give out any personal information about themselves, friends or family

online including home address, phone or mobile phone number
- Never arrange to meet someone they have 'met' on the internet without talking to an adult first; always take an adult and meet in a public place
- Never tell someone they don't know where they go to school, or post any pictures of themselves in school uniform
- Only use a webcam with people they know
- Tell you immediately if they see anything they are unhappy with

Using these rules

Go through these rules with your child. It is a good idea to regularly check the internet sites your child is visiting e.g. by clicking on **History** and **Favourites**.

Please reassure your child that you want to keep them safe rather than take internet access away from them.
For further information go to:
CEOP: www.ceop.gov.uk
Think U Know: www.thinkuknow.co.uk
Childnet: www.childnet-int.org