Values Academy

Online Safety Policy

This statement is part of the suite of documents which contribute to the Safeguarding Policy. It links closely with the anti-bullying policy.

E-Safety encompasses internet technologies and electronic communications such as mobile phones. It is important to educate students about the benefits and risks of using technology and to provide safeguards and awareness for users to enable them to control their on line experience.

E-Safety depends of effective practice at a number of levels:

- Responsible ICT use by all staff and students.

- Sound implementation of the E-Safety policy in both administration and curriculum including secure school network design and use, safe and secure broadband and the effective management of filtering systems.

- The school's E-Safety co-ordinator is the named person at the end of the policy.

Internet use is important as it is an essential element in 21st century life. It is vital for education, business and social interaction. The school has a duty to provide students with quality internet access as part of their learning experience, Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

Internet use will enhance the learning of our students and internet access will be designed for student use and will include necessary filtering

Students will be taught what internet use is acceptable and what is not. It will enrich and extend learning activities. Staff will guide pupils in on line activities that will support learning objectives. It will show effective use of the internet in research, particularly in the skills of knowledge/information location, retrieval and evaluation.

Students will be taught how to evaluate internet content by being aware of the materials they read and how to validate information before accepting accuracy.

If staff or pupils discover unsuitable sites, the URL, date and content must be reported to the Schools Business Manager who will in turn contact Zenzero immediately. All staff must remember that Internet derived materials are subject to Copyright law.

The school pays full regard to the Keeping Children Safe in Education guidelines and is aware that use of technology has become significant in many Safeguarding issues, i.e Child Sexual Exploitation, Radicalisation, sexual preddtion, online bullying and are all addressed when filters are applied. In an attempt to manage online

safety, students do not have wifi access allowing 3G or 4G to be used. We will work with parents/carers to monitor use of mobile data.

Managing and Monitoring Internet Access

- The security of any school information systems will be reviewed regularly (Zenzero).

- Virus protection is installed and updated regularly (Zenzero).

- Strong firewall and filters will be applied.(Zenzero)

- Fastvue monitoring reporting system (Zenzero)

- The schools monitoring and filtering systems comply with UK Safer Internet guidance. Completed documents attached.

E-Mail

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

- There will be no access to personal e-mail accounts or chatrooms while in school.

- Students must be aware of the need to tell a member of staff if they receive offensive e-mail.

- Students must not reveal personal details of themselves in e-mail communications or arrange to meet anyone.

- E-mails sent to an external organisation should be written carefully and authorised before sending.

- There will be no chain letters.

-

The School Website

- The contact details on the Website will be the School address, e-mail and telephone number. Staff or pupils personal information will not be published.

- The CEO will take overall editorial responsibility and ensure that content is accurate and appropriate.

- Written permission from parents or carers will be obtained before photographs are published on the school Website.

Social Networking

- Social networking sites and news groups will be blocked.

- Students will be taught never to give out personal details of any kind which may identify them or their location. Examples will include real name, address, phone numbers, IM address, E-mail address, names of friends, specific interests and clubs.

- Parents will be advised that the use of social network spaces outside school may be inappropriate.

- Inappropriate use of social Networking sites, for example bullying or stalking of another pupil will result in action being taken by the school.

Managing Filtering

- The school will ensure that filtering systems are as effective as possible.

- The School Business Manager will ensure checks are made that filtering is effective.

Managing Video Conferencing (not currently available on either site, but may be accessed elsewhere).

- IP video conferencing should use an educational broadband wherever possible.

- External IP addresses will not be made available.

- Video conferencing will be supervised at all times.

Managing Emerging Technologies

- Emerging Technologies will be examined for educational benefits and a risk assessment will be carried out before use in school is allowed.

Mobile phones

- Mobile phones will not be used during lessons or formal school time.

- The sending of abusive or inappropriate text messages is forbidden and will be subject to the schools discipline procedures.

- Staff will not contact students by personal mobile phones. School phones will be used.

Protecting Personal Data

- Personal Data will be recorded, processed, transferred and made available according to the General Data Protection Regulations May 2018

Authorising Internet Access

- The school will maintain a current record of all staff and students who are granted internet access.

- All staff must read and sign the ICT Acceptable User Policy (AUP) before using any school ICT resource.

Assessing Risks

- Some material available via the internet is unsuitable. Consideration will be given to possible sources when research tasks are set.

- The school will take all reasonable precautions to ensure that users access only appropriate material.

Handling E-Safety complaints

- Complaints of internet misuse will be dealt with by senior members of staff.

- Complaints about staff misuse must be referred to the School Principal.

- Complaints of a Child Protection nature will be dealt with in accordance with the Academy's Child Protection Procedures.

- Sanctions will include removal of internet or computer access for a period of time.

Community use of the Internet

- The school will be aware of internet issues experienced by students out of school and will offer advice

Communications Policy

- Rules for internet access will be posted where there is any ICT provision.

- Students will be informed that internet use is monitored.

- E-Safety will be introduced and reinforced regularly.

- All staff will be aware of the importance of the E-Safety policy.

- Parents will be told of the school policy.

Useful websites

The following website are used as a source of information to support our policy.

Thinkyouknow.co.uk

Saferinternet.org

Childnet.org/cyberbullying-guidance

Educateagainsthate.com

E Safety Co-ordinator is Fiona Hims

Next review; September 2021