ZNANIYE LIMITED

Company: 05254812

E-SAFETY POLICY

2020-2021

Znaniye works alongside the team at the schools in which we operate from as a Supplementary School, and therefore will abide by each schools' own terms for e-safety and IT/technology use. However, Znaniye are committed to ensuring the online safety of students wherever they be, and therefore continue to also implement our own E-Safety rules along side any of those of our locations.

e-Safety is about enabling the school community to benefit as much as possible from the opportunities provided by the Internet and the technologies we use in everyday life. It's not just about the risks, and how we avoid them. It's about ensuring everyone has the chance to develop a set of safe and responsible behaviours that will enable them to reduce the risks whilst continuing to benefit from the opportunities.

An e-safety policy allows the school to demonstrate that not only do we acknowledge e-safety as an important issue for the school community, but also that we have made a considered attempt to embed e-safety into our approach to learning using technology.

An e-safety policy demonstrates how we have worked to achieve a balance between using technology to enhance learning and teaching and putting appropriate safeguards in place. The school's e-safety policy will operate in conjunction with other policies including those for Data Protection, Equality, Disability, Prevent Duty, EYFS and Health and Safety.

Why is Internet use important?

The purpose of Internet use in school is to raise educational standards, to promote student achievement, to support the professional work of staff and to enhance the school's management information and administration systems.

Internet use is part of the statutory curriculum and a necessary tool for learning. It is an essential element in 21st century life for education, business and social interaction. Access to the Internet is

therefore an entitlement for students who show a responsible and mature approach to its use. Our school has a duty to provide students with quality Internet access

Students will use the Internet outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

How does Internet use benefit education?

Benefits of using the Internet in education include:

Access to learning wherever and whenever convenient

Access to world-wide educational resources including museums and art galleries

Educational and cultural exchanges between students world-wide

Access to experts in many fields for students and staff

Professional development for staff through access to national developments, educational materials and effective curriculum practice;

Collaboration across support services and professional associations; Improved access to technical support including remote management of networks and automatic system updates;

Exchange of curriculum and administration data with the SLT and Znaniye + Partners

Responsibilities of the School Community

We believe that e-safety is the responsibility of the whole school community, and everyone has their part to play in ensuring all members of the community are able to benefit from the opportunities that technology provides for learning and teaching. The following responsibilities demonstrate how each member of the community will contribute.

Responsibilities of the Headteacher

Develop and promote an e-safety culture within the school community.

Support the e-safety coordinator in their work.

Make appropriate resources, training and support available to members of the school community to ensure they can carry out their roles with regard to e-safety effectively.

Receive and regularly review e-safety incident logs and be aware of the procedure to be followed should an e-safety incident occur in school.

Take ultimate responsibility for the e-safety of the school community.

Promote an awareness and commitment to e-safety throughout the school.

Be the first point of contact in school on all e-safety matters.

Create and maintain e-safety policies and procedures.

Develop an understanding of current e-safety issues, guidance and appropriate legislation.

Ensure all members of staff receive an appropriate level of training in e-safety issues

Ensure that e-safety education is embedded across the curriculum.

Ensure that e-safety is promoted to parents and carers.

Monitor and report on e-safety issues to Senior Leadership Team as appropriate

Ensure an e-safety incident log is kept up-to-date.

Responsibilities of Teachers and Support Staff

Read, understand and help promote the school's e-safety policies and guidance.

Read, understand and adhere to the school staff Acceptable Usage Policy.

Develop and maintain an awareness of current e-safety issues and guidance.

Model safe and responsible behaviours in their own use of technology.

Embed e-safety messages in learning activities where appropriate.

Supervise pupils carefully when engaged in learning activities involving technology.

Be aware of what to do if an e-safety incident occurs.

Always maintain a professional level of conduct in their personal use of technology .

Responsibilities of Pupils

Help and support the school in creating e-safety policies and practices; and adhere to any policies and practices the school creates.

Take responsibility for learning about the benefits and risks of using the Internet and other technologies in school and at home.

Take responsibility for their own and others safe and responsible use of technology in school and at home, including judging the risks posed by the personal technology owned and used by pupils outside of school.

Ensure they respect the feelings, rights, values and intellectual property of others in their use of technology in school and at home.

Understand what action to take if they feel worried, uncomfortable, vulnerable or at risk whilst using technology in school and at home, or if they know of someone who this is happening to.

Discuss e-safety issues with family and friends in an open and honest way.

Responsibilities of Parents and Carers

Help and support the school in promoting e-safety.

Take responsibility for learning about the benefits and risks of using the Internet and other technologies that their children use in school and at home.

Take responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.

Discuss e-safety concerns with their children, show an interest in how they are using technology, and encourage them to behave safely and responsibly when using technology.

Model safe and responsible behaviours in their own use of technology.

Consult with the school if they have any concerns about their children's use of technology.

Learning and Teaching

We believe that the key to developing safe and responsible behaviours online, not only for pupils but everyone within our school community, lies in effective education. We know that the Internet and other technologies are embedded in our pupils' lives not just in school but outside as well, and we believe we have a duty to help prepare our pupils to safely benefit from the opportunities the Internet brings.

We will discuss, remind or raise relevant e-safety messages with pupils routinely wherever suitable opportunities arise during all lessons; including the need to protect personal information, consider the consequences their actions may have on others, the need to check the accuracy and validity of information they use, and the need to respect and acknowledge ownership of digital materials.

School will ensure that the use of Internet derived materials by students and staff complies with copyright law

Students will be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy

Staff will model safe and responsible behaviour in their own use of technology during lessons.

Managing ICT Systems and Access

The school will be responsible for ensuring that access to the ICT systems is as safe and secure as reasonably possible on all their campuses. Znaniye will ensure to have an IT contact at all of their branches to deal with any issues and queries and allow access when required

Servers and other key hardware or infrastructure will be located securely with only appropriate staff permitted access.

Servers, workstations and other hardware and software will be kept updated as appropriate.

The school will agree which users should and should not have Internet access, and the appropriate level of access and supervision they should receive.

Users will be made aware that they must take responsibility for their use of, and behaviour whilst using, the school ICT systems, and that such activity will be monitored and checked.

Wireless Access

Wireless access to the network is provided in certain areas of the school. The school is responsible for ensuring that access is safe and secure as reasonably possible.

Connection to the wireless network is protected by at least the Wi-Fi Protected Access (WPA) authentication method requiring the input of a secure passphrase.

Using new technologies

As a school we will keep abreast of new technologies and consider both the benefits for learning and teaching and the risks from an e-safety point of view.

We will regularly amend the e-safety policy to reflect any new technology that we use, or to reflect the use of new technology by pupils which may cause an e-safety risk.

Protecting personal data

We will ensure personal data is recorded, processed, transferred and made available according to the Data Protection Act 1998.

Staff will ensure they properly log-off from a computer terminal after accessing personal data.

Staff will not remove personal or sensitive data from the school premises without permission of the headteacher, and without ensuring such data is kept secure.

All staff will be aware of and have access to the Data Protection policy.

The school website and other online content published by the school

The school website will not include the personal details, including individual e-mail addresses or full names, of staff or pupils.

A generic contact e-mail address will be used for all enquiries received through the school website.

All content included on the school website will be approved by the Directors.

The content of the website will be composed in such a way that individual pupils cannot be clearly identified.

Staff and pupils should not post school-related content on any external website without seeking permission first.

Communication of Policy

Pupils

Pupils will be informed that Internet use will be monitored.

Staff

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

Parents

Parents/Carers' attention will be drawn to the school e-Safety Policy and Acceptable Usage Policy in the school prospectus and on the school website.

Dealing with breaches of ICT Policy

accessing illegal content deliberately

accessing inappropriate content deliberately

accessing other non-educational websites (e.g. gaming or shopping websites) during lesson time

sharing your username and password with others

opening, altering, deleting or otherwise accessing files or data belonging to someone else

failure to abide by copyright of licensing agreement

Whilst resolving an incident those students involved may have their computer accounts suspended.

Examples of possible e-safety incidents involving pupils:

accessing illegal content accidentally and failing to report this

accessing inappropriate content accidentally and failing to report this

inappropriate use of personal technologies (e.g. mobile phones) at school

accessing social networking sites, chat sites, instant messaging accounts or personal email where not allowed

downloading or uploading files not allowed

accessing school ICT systems with someone else's username and password

using school or personal equipment to send a message, or create content, that is offensive or bullying in nature

attempting to circumvent school filtering, monitoring or other security systems

sending messages, or creating content, that could bring the school into disrepute

revealing the personal information (including digital images, videos and text) of others by electronic means (e.g. sending of messages, creating online content) without permission

use of online content in such a way as to infringe copyright or which fails to acknowledge ownership (including plagiarising of online content)

Examples of possible e-safety incidents involving staff:

transferring personal data insecurely

using digital communications to communicate with pupils in an inappropriate manner (for instance, using personal email accounts, personal mobile phones, or communicating via social networking sites)

Where a member of staff is made aware of a possible e-safety incident, they should inform Headteacher who will then use the schools agreed procedure to respond in the most appropriate manner.

Znaniye Limited

52 Mayfield Gardens

W7 3RH

school@znaniye.com

07769313090