THE RICHARD PATE SCHOOL

E-Safety Policy

Sept 2019

Introduction

'*At the Richard Pate School we consider the teaching of e-Safety to be an important part of the curriculum for all pupils, not only in terms of how to avoid pitfalls when using technology now, but also equipping them to be resilient digital citizens of the future'.*

This guidance is applicable to all those involved in the provision of e-based education and resources at the School and those with access to, or are users of, School ICT systems. It is part of the wider safeguarding agenda and outlines how we will work to ensure our school is prepared to deal with the safety challenges which prevail in the modern world.

Definition of e-Safety

E-Safety serves to raise awareness and understanding of the potential dangers and risks associated with the use of the Internet, mobile phones, tablets and game consoles etc. both in and beyond School.

The elements of e-Safety are listed in Appendix 1.

We aim to:

- ensure that staff and pupils recognise the risks associated with the use of technology and how to deal with them
- ensure that pupils are appropriately supervised during school activities
- promote responsible behaviour with regard to e-based activities
- take account of legislative guidance
- make all staff and pupils aware of the procedures for reporting incidents relating to e-Safety e.g. cyberbullying etc.

Responsibilities

The Headmaster and the DSLwill be responsible for the implementation of this policy.

The E-Safety Coordinator (MG) will:

- Keep up to date with E-safety issues (e.g. via CEOPS)

- report to the Headmaster and the school's Designated Safeguarding Leader (SW) of any incidents
- ensure that staff have read this Policy (use of signing off procedure)

- provide/arrange for staff training (assemblies and INSET)
- liaise with the school's network manager
- liaise with the Headmaster on any investigation and action in relation to e-Safety incidents
- follow up/track any incidents/issues and check they are logged in the pupils' profiles section of the School Manager System
- attend relevant courses relating to e-Safety
- draft and review the Policy for e-Safety
- source and provide any necessary e-Safety resources for teachers
- Help to impose sanctions on pupils where appropriate (linked to Behaviour Policy)

The E-Safety Co-ordinator together with the Network Manager (DH) will:

- be responsible for the IT infrastructure and that it is not open to misuse or malicious attack
- ensure that users may only access the networks and devices through an enforced password protection system/routine
- keep up to date with e-Safety technical information in order to carry out their role
- ensure that the use of the network (including internet, virtual learning, email and remote access) is monitored for misuse
- implement any agreed monitoring, filtering or blocking software/systems – *Barracuda Web Filter, Google Safe Search facility and the monitoring of emails by pupils*
- Liaise with the DSL

Teaching and Support Staff (including Supply Staff) will:

- maintain awareness of school e-Safety policies and practices
- impose sanctions through discussion/negotiation with MG, RM, SW (Linked to Behaviour Policy)
- attend assemblies and/or staff meetings which relate to e-Safety (where appropriate)
- report immediately on any incidents to MG, RM or SW
- ensure that all digital communications with pupils, parents, carers and fellow staff are on a professional level (See Behaviour Policy and Anti Bullying Policy)
- not engage with pupils on social media (See Staff Employment Handbook for more details on using social media)
- include e-Safety in relevant teaching activities and curriculum delivery differentiated as appropriate
- ensure pupils understand and follow e-Safety policies, including the need to avoid plagiarism and uphold copyright regulations
- monitor the use of digital technologies (including mobile devices, cameras etc.) during school activities
- ensure that where the use of the internet is pre-planned, pupils are guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- ensure that the 'Acceptable use of the Internet' rules for pupils are displayed in their work areas and are reinforced with the pupils on a regular basis

Child Protection

Staff should be aware of e-Safety issues and the types of risk online including:

- sharing of personal data
- access to illegal/inappropriate materials
- inappropriate contact on-line with adults/strangers

- potential or actual incidents of grooming
- cyber-bullying
- sexting

Staff should be aware that e-Safety also features in the following school policies and why:

- *Safeguarding Policy – including Staff Code of Conduct*
- *Anti-Bullying Policy*
- *Behaviour Policy*
- *Policy on Taking, Storing and Using Images of Children*

Pupils

- will understand the consequences of the misuse of mobile phones, tablets and other devices which have connectivity or video recording functions etc.
- will understand the sanctions which will be imposed if they breach the rules (linked to Behaviour Policy)
- will understand the importance of reporting abuse, misuse or access to inappropriate materials, etc
- will know to report any incidents (including on behalf of one of their peers) to their class teacher, the E-Safety Co-ordinator (MG) or to any other trusted adult in School or at home
- will understand that the e-Safety policy will include actions outside of School where related to School activities e.g. misuse of digital cameras on school trips
- will not bring any personal electronic devices to school, including phones, tablets or digital cameras (unless permitted by their teacher)
- read and sign an agreement regarding e-Safety rules (Years 3 to 6)
- be able to retain/recall and understand the SMART rules including ZIP IT, Block IT and Flag IT (see e-Safety resources in Teacher shared area of network and posters dotted around the School)
- be aware of the reasons why there are recommended age restrictions for computer games and digital films etc.

Parents/Carers – Raising awareness

- will be advised of any relevant e-Safety matters by means of parents' evenings, newsletters, e-mails and the School's website etc.
- will be made aware of external E-Safety resources e.g. Internetmatters.org
- countersign pupils' e-Safety agreement in (Years 3 to 6)
- will be encouraged to support the School in the promotion of good e-Safety practice
- should follow school guidelines on:

    - digital and video images taken at School events
    - access to parents' sections of the School website and pupil records etc.
    - their children's personal devices in the School (where this is permitted)

Community Users

Where such groups have access to school networks and devices, Community Users will be expected to abide by School e-Safety policies and procedures. This includes Trustees, members of the PTA and Supply Teachers.

Appendix 1. The Elements of E-Safety

Safety: Children learn that to enjoy and explore what the internet can offer, and to collaborate with others, they need some more advanced advice to stay safe. They build on the smart rules to help them do this. Their understanding and recognition of risk grows and develops with age.

For your information, the SMART rules are in poster form in this link:

http://www.kidsmart.org.uk/downloads/cn_A2posterPRIMARY.pdf

Privacy: Pupils learn several ways to keep their privacy protected. They understand what constitutes personal information and they learn about usernames and the use of strong passwords. They understand why they need to take these steps and how to refuse requests to provide personal information.

Safe Search: They learn to search for information and to question the credibility and accuracy of search results and information they obtain online. They evaluate and compare material. They know there are inappropriate and harmful websites.

Copyright: They know they must acknowledge the owner of the work and not copy and paste information as if it is their own work. They learn to interpret what they find in their own words and credit the original where needed. They understand that the creator of the work has ownership.

Digital Footprint: They learn to be careful about what they upload or say online and respect their own and others' privacy. They understand that material they post or upload can be around for years for others to find, leaving a permanent digital footprint. They learn to protect photos they do decide to upload or post and to show judgement about acceptable use of new technology.

Cyberbullying: They learn to treat one another with respect. They understand what to do if they experience aggression or cyberbullying online and they help their friends if they experience this. They work to prevent bullying in their setting.

Safe Relationships: They learn to make safe relationships, understand that friendship online can be very different to friendships offline. They understand the risks of unsafe contact. They know how to get help if anything worries them or makes them uncomfortable online. They can report abuse.

Downloads: They learn about download risks and how to be aware of scams, phishing, viruses and unsafe attachments. They can recognise and distinguish adverts from content. They can successfully download legitimate material and work with it using different software programmes.

Uploads: They learn to post photos and comments online selectively and with care, and to take steps to ensure photos are protected. They understand privacy settings and tags. They do not use photos of other people disrespectfully.

Safe Play: They understand the risks when playing online games, they are aware of the risk when in contact with players that they have never met and can confidently take themselves out of a game or chatroom and report any problems to an adult. They play games appropriate for their age.

Safe Shopping: they look for trusted online retailers, they check security symbols and the URL before using a family credit card. They can use PayPal. They learn that apps and games could have hidden costs despite being free to download first.

Safe Phones: They learn to use their mobile phones safely. They understand location services. They use messaging apps and services but know they should not pass on bullying, rumours about other people or threatening messages. If they are contacted by anyone they do not know or feel uncomfortable about anything, they know how to seek help. Phones should not be used for cyberbullying.

Safe Talk: This covers all forms of communication including text, messaging, emailing, chat and apps as well as chat in games and phone calls. They learn to communicate and collaborate safely and appropriately with others online. They learn to recognise risky situations and know how to block a sender, save evidence and get help. Safe Talk includes safe social networking and groups.

Secure Users: All these components contribute to: Secure, competent and confident web users, taking on new devices, new software and apps and conducting themselves safely.