Rowley Park
Primary Academy

Computing
&
E-Safety Policy

2017-2018

Updated October 2017

1. Writing and reviewing the e-Safety policy

Electronic safety (or e-Safety) is not just about keeping safe on the internet but includes all electronic devices including mobile phones, computers, tablets and television.

The e-Safety Policy links to other school policies including those for ICT and safeguarding (Anti-Bullying, Health and Safety and Child Protection).

Our e-Safety Policy has been written by the school, building on existing best practice guidance. Parents, pupils, staff and governors have been consulted in the development of the policy.

The school ICT leaders (Helen Stubbs) will assume the role of e-Safety coordinators. It is an important role that requires close liaison with the Designated Safeguarding Lead (Helen Stubbs). It is not a technical role.

The e-Safety policy and its implementation will be reviewed annually.

Impact of the e-safety policy will be monitored through:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited) / filtering
- Internal monitoring data for network activity
- Pupil/parent /staff voice

2. Teaching and Learning

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 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. All pupils will be required to access the World Wide Web on a regular basis.

<u>Internet use will enhance learning</u>

The school Internet access will be designed expressly for pupil use and will include 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 safe Internet use.

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

<u>Pupils will be taught how to evaluate Internet content</u>

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

A planned online safety curriculum should be provided as part of Computing / PHSE /other lessons and should be regularly revisited. It will include:

- Key online safety messages should be reinforced as part of a planned programme of assemblies and computing lessons

- pupils will be taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information.

- pupils will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet

- pupils should be supported in building resilience to radicalisation by providing a safe environment and helping them to understand how they can influence and participate in decision-making.

- Staff will act as good role models in their use of digital technologies the internet and mobile devices

- In lessons where internet use is pre-planned, pupils will be 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.

- Where pupils are allowed to freely search the internet, staff will be vigilant in monitoring the content of the websites the young people visit.

- It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study.

3. **Managing Internet Access**

Information system security

The School ICT systems' capacity and security will be reviewed regularly. Virus protection will be updated regularly.

Security strategies will be monitored by the school network manager, ICT leader, e-Safety governor and leadership team.

Email

Pupils may only use approved authorised email accounts - group or individual – that are part of the school network. Pupils are not to use their own personal/family accounts.

Pupils must immediately tell a teacher if they receive offensive emails.

Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone.

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

The forwarding of chain letters is not permitted.

Published content and the school web site

The contact details on the school website should be the school address, email and telephone number. Staff or pupils' personal information will **not** be published.

The head of school will take overall editorial responsibility and ensure that content is accurate and appropriate to the best of her ability.

Publishing pupils' images and work

Photographs that include pupils will be selected carefully and **will not** enable individual pupils to be clearly identified.

Pupils' full names, and other personal details that can identify a child, will not be used anywhere on the website or E-portal (learning platform -public area), particularly in association with photographs.

Written permission from parents or carers will be obtained before photographs of pupils are published on the school website or Learning Platform (public area) on admission to the school, as part of the e-Safety Agreement.

The school retains all intellectual rights to any school-related work published.

Social networking and personal publishing

The school will use Social Networking Sites such as Twitter for the purpose of school and its affiliated activities. Network sites, by pupils and staff will not be used for personal correspondence.

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

Pupils and parents will be advised that the use of social network sites outside school is inappropriate for primary aged pupils.

Managing filtering

The school will work with the internet provider to monitor and filter websites and its contents.
If pupils discover an unsuitable site, it must be reported to a member of staff who in turn should refer the matter to the e-Safety coordinator or Head of School. If staff access an unsuitable site then the e-Safety coordinator should be informed immediately. In both cases, the e-Safety coordinator will arrange for access to the site to be blocked. Children will be taught what to do if an unsuitable site or 'pop-up' appears on the screen (turn screen off and report immediately to the teacher, who will obtain the address and report to the e-Safety coordinator as above).

The e-Safety leader (through the network manager) will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Internet filtering should ensure that children are safe from terrorist and extremist material when accessing the internet.

The academy has provided differentiated user-level filtering (allowing different filtering levels for different ages / stages and different groups of users – staff / pupils / students etc)

Managing new and emerging technologies (including mobile phones)

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

The use of portable media such as iPads, mobile phones etc. will be monitored closely as potential sources of computer virus and inappropriate material.

If a pupil brings a mobile phone into school (for security purposes i.e.: Year 5 /6 pupils walking to/from school without an adult) the mobile will be handed in at the office and collected at the end of the school day. Pupils are **not** allowed to bring mobile phones into the classroom. If they do, the mobile phone will be confiscated by teaching staff at morning registration and returned to the **pupil's parent** at the end of the school day. The school accepts no responsibility for loss or damage to pupils' phones however caused. Being in possession of a mobile phone in the classroom is in breach of the school discipline policy.

The sending of abusive or inappropriate text messages is forbidden.

Mobile devices not owned by the school may **not** be used to photograph any pupil including for the use of social media (Twitter)

Staffs use of mobile phones is done so under professional conduct (refer to Staff Handbook)

Protecting personal data

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

4. Policy decisions

Authorising Internet access

Pupil instruction in responsible and safe use should precede **any** Internet access and all pupils must sign up to the Pupil e-Safety Agreement to abide by the school's e-Safety rules. These e-Safety rules will also be displayed clearly in all classrooms. Failure to abide by these rules may constitute a breach of the school discipline policy.

Where practicably possible, all pupil access to the internet will be supervised by an adult, using approved on-line materials. Older children (upper key stage 2, but at the discretion of the teacher) will on occasions be indirectly supervised if they are completing an independent task, set by the teacher.

All parents will be asked to sign the Parent e-Safety Agreement confirming that they will comply with this policy ensuring that their child follows to the best of his or her ability the school e-Safety rules.

All staff must read and agree in writing to adhere to the Acceptable Use Agreement for Staff before using any school ICT resource.

Assessing risks

The school 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 a school computer.

The school will audit ICT provision regularly to establish if the e-Safety Policy is adequate and that its implementation is effective.

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 Head of School and dealt with in accordance with Staffordshire Authority complaints procedures.
Complaints of a child protection nature must be dealt with in accordance with school child protection procedures (Please refer to Safeguarding and Child Protection).

Community use of the Internet

External organisations using the school's ICT facilities must adhere to the e-Safety Policy.

5. Communications Policy

Introducing the e-Safety Policy to pupils

E-Safety rules will be posted in all classrooms and discussed with the pupils at the start of each year.

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

Staff and the e-Safety Policy

All staff will be given a copy of the School e-Safety Policy and are expected to have read it and understood its contents.

Any information downloaded must be respectful of copyright, property rights and privacy.

Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

A laptop/iPad issued to a member of staff remains the property of the school. Users of such equipment should therefore adhere to school policy regarding appropriate use with regard to Internet access, data protection and use of software (Social Media Policy).

Enlisting parents' support

Parents' attention will be drawn to the school e-Safety policy in newsletters, on the learning platform and the school website.

6. Monitoring and review

This policy is implemented on a day-to-day basis by all school staff and is monitored by the e-Safety Coordinators.

This policy is the Governors' responsibility and they review its effectiveness annually. They do this during reviews conducted between the e-Safety coordinator, ICT coordinator, Designated Safeguarding Lead, Governor with responsibility for ICT and Governor with responsibility for Safeguarding. Ongoing incidents would be reported to the full governing body.

The e-Safety Policy was revised by the **e-Safety coordinator Miss Helen Stubbs (DHT)**

Date revised: October 2017

Signed: …… (Headteacher)

Approved by the Governing Body of Rowley Park Primary Academy.

Signed: …… (Chair of Governors)

Date: .....

Appendix 1: Staff Code of Conduct for ICT

To ensure that members of staff are fully aware of their professional responsibilities when using information systems and when communicating with pupils, they are asked to sign this code of conduct. Members of staff should consult the school's e-safety policy for further information and clarification.

- I understand that it is a criminal offence to use a school ICT system for a purpose not permitted by its owner.
- I appreciate that ICT includes a wide range of systems, including mobile phones, PDAs, digital cameras, email, social networking and that ICT use may also include personal ICT devices when used for school business.
- I understand that school information systems may not be used for private purposes without specific permission from the Head of School
- I understand that my use of school information systems, Internet and email may be monitored and recorded to ensure policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone other than an authorised system manager.
- I will not install any software or hardware without permission.
- I will ensure that personal data is stored securely, using the encryption software, and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will respect copyright and intellectual property rights.
- I will report any incidents of concern regarding children's safety to the e-Safety Coordinators, the Designated Child Protection Coordinator or Head of School
- I will ensure that electronic communications with pupils and parents, including email, IM and social networking are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.
- I will promote e-safety with students in my care and will help them to develop a responsible attitude to system use, communications and publishing.
- The school may exercise its right to monitor the use of the school's information systems and Internet access, to intercept e-mail and to delete inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

I have read, understood and accept the Staff Code of Conduct for ICT.

Signed: …… Date:……..

Rowley Park Primary Academy
Pupil Acceptable Usage Policy and e-Safety Pledge

All pupils will follow the conditions described in this policy when using school computer networked resources including: Internet access and our school's Learning Platform both in and outside of school.

Breaking these conditions may lead to:

- Withdrawal of the pupil's access
- Close monitoring of the pupil's network activity
- Investigation of the pupil's past network activity
- If necessary and applicable, criminal prosecution

Pupils will be provided with guidance by staff in the use of the resources available through the schools network.
Our IT Technician will regularly monitor the network to make sure that it is being used responsibly.

Conditions of Use
Pupil access to the networked resources is a privilege, not a right. They will be expected to use the resources for the educational purposes for which they are provided. It is the personal responsibility of every pupil to take all reasonable steps to make sure they follow the conditions set out in this Policy.
They must also report any misuse of the network to their Class Teacher/Senior Leader.

ACCEPTABLE USE
Pupils are expected to use the network systems in a responsible manner. It is not possible to set a complete set of rules about what is, and what is not, acceptable. All use however should be consistent with the school ethos and code of conduct.

In the Early Years Foundation Stage and Key Stage 1 all pupils will be expected to follow our school's e-Safety rules which are shared verbally and displayed near computer equipment.
As pupils enter Key Stage 2 they will be expected to follow our school's e-Safety rules which are shared verbally and displayed near computer equipment as well as having to read/have read to them and sign our Key Stage 2 e-Safety Pledge.

The Pupil Acceptable Usage Policy is part of wider Safeguarding Policy procedures and information across the school. It is linked to our Safeguarding Policy, Anti-Bullying Policy, e-Safety Policy and Staff and Parent Acceptable Usage policies.

Rowley Park
Primary Academy

Key Stage 2 e-Safety Pledge

I understand this e-Safety pledge, once signed, will last for the entire time I spend in Key Stage 2.


I will be polite on line and remember that I am a pupil that represents Rowley Park Primary Academy.


I will not make, send or post any material that is likely to upset other children or adults.


I understand the school network is monitored regularly by our IT Technician and the Head of School will be told if there is a problem.


I will not reveal any personal information (e.g. home address, telephone number) about myself or other users over the network or enter into other users' files or folders.


I will not share my login details (including passwords) with anyone else and will never use other people's username and password. I will log off any machine in another users name and re-log in using my name.


If I think someone has learnt my password then I will tell my class teacher immediately and make sure I log off after my network session has finished.


I understand that I am not allowed access to any type of chat room and will not try to gain access to them.


I will not use or bring into school, any type of electronic equipment/mobile phone/ipad etc. without permission.


I will not attempt to harm or destroy any IT equipment or the work of another user or website connected to the school system.

I will report any accidental access to other people's information, unsuitable websites or being sent anything that makes me feel uncomfortable to my class teacher.


I will not attempt to download and/or install any unapproved software or resources from the Internet.


I will follow the instructions and guidance about e-Safety given to me by staff at school in all lessons across the curriculum and if I have access to IT equipment at other times.