Race Leys
Junior School

E-Safety Policy

Date: 09/2018
Review Due: 09/2019

Reviewed Annually

Race Leys Junior School's lead professional for day to day E-Safety is Martyn Hole, reporting directly to Suzanne Edwards (head)

This policy has been written for Race Leys Junior School, in line with local and national guidance.

This policy should be read in conjunction with the Safeguarding and Child Protection Policy, the Anti-bullying Policy and the PSHE policy.

Background

At Race Leys Junior School we understand the benefits and the risks associated with using the internet. This policy sets out clear procedures to ensure our pupils are safe and that they can learn how to use the Internet and ever changing technologies in a safe and discerning way.

Adults, as well as young people, can find themselves vulnerable to malicious use of the Internet both in their personal and professional lives. This policy highlights the importance of training and guidance in good practice in safer use of the Internet for staff. The policy also recognises that there are other safety issues associated with using technologies, such as over-exposure to LCD screens, privacy etc.

The Internet and associated technology is a rapidly evolving environment where new opportunities and risks appear daily. Pupils learn to manage existing risks and understand the dynamic nature of technologies, so that they are able deal confidently with challenges in the future, whatever they might be.

1. Teaching and learning

As we move towards a more digital curriculum, we will actively promote the use of 'real-world' technologies to enhance and support learning.

1.1 Why internet use is important

- 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.

1.2 Internet use will enhance learning

- The school's internet access has been designed expressly for pupil use and includes filtering appropriate to the age of pupils. This screening and blocking is operated centrally by Warwickshire LA IT services.
- Pupils will be taught the differences between acceptable and unacceptable Internet use and given clear objectives for Internet use.
- The school is vigilant in its supervision of pupils' use at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas where

older pupils have more flexible access.

- In the event of pupils trying to make inappropriate use of the internet, particularly using search engines, this is captured and reported in real time by Warwickshire IT services. Senior staff will follow these up with pupils, notify their families and keep an incident record on the pupil's file for future reference as required.
- Pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation both in mainstream lessons and as part of the IT curriculum in each year group.

Good Practice

- Teachers will update and check websites before accessing with the children to ensure that the content is appropriate. The curriculum is planned in context for internet use to match pupils' ability, using child-friendly search engines where more open Internet searching is required; e.g. Yahoo for kids or Ask for kids
- Families provide consent for pupils to use the internet, as well as other ICT technologies, as part of the e-safety acceptable use agreement form at time of their child's entry to the school.
- The school makes clear all users know and understand what the 'rules of appropriate use' are and what sanctions result from misuse – through staff meetings and the curriculum plans.
- A record is kept of any cyberbullying or inappropriate behaviour in-line with the school behaviour management system. Parents/carers are informed of significant or repeated inappropriate behaviours.
- The school ensures the Designated Safeguarding Lead Professional has appropriate training in E-Safety training.
- The school provides advice and information on reporting offensive materials, abuse/ bullying etc and makes this available for pupils, staff and parents.
- E-Safety advice for pupils, staff and parents is provided annually.
- The school ensures that when copying materials from the web, staff and pupils understand issues around plagiarism; how to check copyright and also know that they must observe and respect copyright / intellectual property rights.
- The school ensures that staff and pupils understand the issues around aspects of the commercial use of the internet, as age appropriate. This may include, risks in pop-ups; buying on-line; on-line gaming / gambling.
- The school makes training on the E-Safety education available to staff
- The school gives advice, guidance and training for parents, including information leaflets; practical sessions; in school newsletters; on the school web site;

1.3 Pupils will be taught how to evaluate internet content

- The school will ensure that the use of internet derived materials by staff and pupils

complies with copyright law.

- Pupils are taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Race Leys has a clear, progressive e-safety education programme throughout all Key Stages, built on local and national guidance. Pupils are taught a range of skills and behaviours appropriate to their age and experience, such as:

- to STOP and THINK before they CLICK
- to discriminate between fact, fiction and opinion
- to develop a range of strategies to validate and verify information before accepting its accuracy
- to skim and scan information
- to be aware that the author of a web site / page may have a particular bias or purpose and to develop skills to recognise what that may be
- to know how to narrow down or refine a search
- [for older pupils] to understand how search engines work and to understand that this affects the results they see at the top of the listings
- [for older pupils] to understand 'Netiquette' behaviour when using an online environment / email, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private
- [for older pupils] to understand how photographs can be manipulated and how web content can attract the wrong sort of attention
- [for older pupils] to understand why on-line 'friends' may not be who they say they are and to understand why they should be careful in online environments
- [for older pupils] to understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have turned-on privacy settings
- [for older pupils] to understand why they must not post pictures or videos of others without their permission
- [for older pupils] to know not to download any files – such as music files --- without permission
- [for older pupils] to have strategies for dealing with receipt of inappropriate materials
- [for older pupils] to understand online purchasing e.g. apps and within app purchases
- [for older pupils] to understand why and how some people will 'groom' others with inappropriate or illegal motives

2. Managing Internet Access

2.1 Information system security

- School ICT systems capacity and security are reviewed regularly
- Virus protection is updated regularly.

2.2 E-mail

- Pupils may only use approved school e-mail accounts on the school system.
- E-mails 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.

2.3 Published content and the school website

- The contact details on the website are the school address, e-mail and telephone number. Staff, pupils' or governor's personal information will not be published.

- The Head will take overall editorial responsibility and ensure that content is accurate, appropriate, up to date and aligned to statutory requirements regarding information that schools must have on their website as determined by the DfE.

- The school website is managed externally by an independent provider contracted by the Griffin Schools Trust; all website material must be in line with GST formats and guidelines.

2.4 Publishing pupil's images and work

- Photographs that include pupils will not refer to the pupil by name. Digital images /video of pupils stored in a teacher's documents or shared images folder on the network are deleted at the end of the year – unless specifically required for a key school publication or assessment information.

- Images of children and staff are not to be taken on or away from school premises by parents or visitors, unless prior permission is explicitly sought and given by the school or at scheduled school events such as assemblies or festivals.

- Pupils are not identified by their full name in online photographic materials in the credits of any published school produced video materials / DVDs.

- Parental agreement is obtained, through the specific comfirmation of consent form signed at point of admission, before pupils images are published on the school's website or other publications e.g. local newspapers.

- Staff are not allowed to use mobile phones / personal equipment for taking pictures of pupils.

- Pupils are taught about how images can be manipulated in their E-Safety education programme and also taught to consider how to publish for a wide range of audiences, which might include governors, parents or younger children.

2.5 Social networking and personal publishing

- The school blocks/filters access to social networking sites or newsgroups unless there is a specific, approved educational purpose.

- Pupils are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.

- Newsgroups will be blocked unless a specific use is approved.

- Pupils are advised never to give out personal details of any kind which may identify them or their location.
- Pupils and parents are advised that the use of some social network spaces, for example Facebook, Bebo, MySpace outside school is inappropriate for primary aged pupils and that some of these sites have minimum age requirements.
- Pupils are taught that they should not post images or videos of others without their permission. They are taught about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location, such as house number, street name or school. They are taught the need to keep their data secure and what to do if they are subject to bullying or abuse.

2.6 Managing filtering

- The school will work with relevant providers (in this case Warwickshire LA) to ensure systems which protect pupils are regularly reviewed and improved.
- If staff or pupils discover an unsuitable site, it must be reported to the E-Safety Leader. Concerns are escalated to the Technical Service provider as necessary.
- The school will immediately refer any material we suspect is illegal to the appropriate authorities e.g. Police, and the local authority.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

2.7 Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.

2.8 Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the 2018 GDPR requirements

3. Policy Decisions

3.1 Authorising Internet access

- The school reserves the right to withdraw internet access from a pupil or member of staff in the event of misuse or infringement of policy.

3.2 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 can accept liability for the material accessed, or any consequences of Internet access.

- The school will audit ICT provision annually to establish whether the E-Safety policy is adequate and that its implementation is effective.

3.3 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.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Discussions will be held with the Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues.

4. GDPR – 2018 compliance

The aim of GDPR legislation is to return control to individuals by allowing them to request deletion or disclosure of their data. As a school we have a responsibility to provide evidence of our data storage activities. In terms of E-Safety the implications of this are as follows:

- The school must annually ensure that its digitally held (and paper based) storage of personal data is logged and that a list of the software used across school (including teacher selected APPs) are GDPR compliant.
- Staff need to check what data is being extracted by all online tools / APPs used and that this is in line with GDPR requirements
- The school must have a lawful basis for processing personal data
- Parents must complete a data use consent form each year
- The school must have a privacy policy on the website, which must be distributed to all staff
- There should be clear procedures in place to find, delete and disclose relevant data as required. Warwickshire IT services provide a helpdesk service for schools regarding the legal and timeliness of data deletion.
- The school has a clearly defined process for Subject Access Requests which is published on the website
- The school must appoint a data Protection Officer – in 2018/9 this is Martyn Hole.

5. Communications Policy

a. Introducing the E-Safety policy to pupils

i. E-safety rules are displayed in all classrooms and other work areas and are discussed with the pupils on a regular basis.
ii. Pupils are informed that network and internet use will be monitored.
iii. Pupils are not allowed to use mobile phones in school.

b. Staff and the E-Safety policy

i. The E-Safety Policy is distributed to all staff and is included in child protection training sessions.
ii. Internet usage is able to be monitored and can be traced to the individual user.
iii. Discretion and professional conduct is essential.

c. Enlisting parents' support

Parents/carers' attention will be drawn to the school E-Safety Policy in a variety of ways including: newsletters, open evening events and on the school Web site.

A range of resources and activities are available through:

i. CEOP – Child Exploitation and Online Protection
ii. http://www.thinkuknow.co.uk/5_7/
iii. https://www.thinkuknow.co.uk/Teachers/Lee-And-Kim/
iv. http://www.thinkuknow.co.uk/8_10/
v. https://www.thinkuknow.co.uk/teachers/resources/?tabID=2