Rickley Park

Cracking the Code of Learning Together

E-Safety and Internet Access Policy

Date of Policy: January 2022
Date of Review: January 2023

1. Key Values

- We have the same chances. We have the same choices.
- We know that everyone has something special to contribute.
- We persevere and work hard, not because we are told to but because we want to improve.
- We stick together for the good of all.
- We look after ourselves, each other and our world by taking responsibility for our actions.
- We let everybody talk and have their say.

2. Introduction – Why is Internet Access important?

The E-safety and Internet Access Policy should be read in conjunction with the schools' behaviour, bullying and child protection policies.
This policy covers Internet access at school, as well as guidance given to pupils and parents for E-safety when accessing the Internet when not at school.
Wherever "staff" are referred to during this policy this refers to all paid employees, any volunteer staff (e.g. student teachers, work experience) and governors.

2.1 The Internet has become increasingly important in our society and is essential for education, business and social interaction. Internet use is part of the statutory curriculum and a necessary tool for all staff and pupils. It links and enhances all areas of the curriculum, with a wide range of uses including for research and interaction with educational games. The school has a duty to ensure that every child in our care is safe, and the same principles should apply to the "digital" world as would be applied to within the school's physical buildings.

3.Learning.

3.1 Internet use will enhance and accelerate learning.

- The school Internet access is designed expressly for pupil use and includes filtering appropriate to the age of pupils alongside monitoring of its use (managed by our ICT technician and Computing Lead) Our filtering system complies fully to DfE requirements.
- Pupils are taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Pupils are educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- Pupils have access to a Gmail account, which is managed by Rickley Park, to ensure communication within a "safe platform."
- Pupils are shown how to publish and present information to a wider audience.
- Pupils are taught how to effectively communicate online in real-time to enhance and work collaboratively on projects.
- Pupils are shown how to access on-line learning environments using google or apple apps.
- The school ensures that apps used are fully compliant with GDPR, with companies asked to provide the relevant documentation.

3.2 Pupils are 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. This will include how to acknowledge the source of information when it is extracted from the Internet.

- Pupils will be taught the importance of cross-checking information to ensure validity before accepting its accuracy.
- Pupils will be taught about the importance and integrity of avoiding plagiarism.

3.3 Pupils are taught about E-safety.

- E-safety and cyber-bullying will be covered in lessons, both within the Computing and RSHE curriculum
- Pupils will be taught about what to do if they come into contact with inappropriate materials on the Internet.
- Pupils (and parents) will be reminded that negative comments made about each other via the Internet and emails are not accepted by the school.

4. Managing Emerging Technologies.

Technology continually evolves. Access is becoming increasingly more mobile and universally used. The school will take every opportunity to enhance learning within the classroom. Emerging technologies will be evaluated for educational benefit and a risk assessment will be carried out before use in school is allowed.
Mobile phones will not be used for personal use, by pupils and staff during lessons.

5. Internet Access.

The school will take all reasonable precautions to prevent access to inappropriate 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 device connected to the school's network or Internet. The school cannot accept liability for any material accessed, or any consequences of Internet access. (*See "Parent Internet Consent Form" Appendix 1*)
In order to prepare pupils to be successful citizens it is imperative to teach them how to assess and manage their own e-safety risks. Ofsted states that "in schools that had "managed" systems pupils have better knowledge and understanding than those that use a "locked down system." Whilst the school takes all reasonable precautions, we do not believe that limiting Internet access to bookmarked websites teaches children these necessary life-skills. Our aim is to provide opportunities to enable pupils to learn how to risk-assess to enable richer learning experiences when using online tools.
The use of websites such as You-Tube are to be accessed cautiously making sure that staff and pupils are aware of the potential risks of being exposed to inappropriate material and that they know how to deal with such a situation. Access to "You-Tube" for pupils is automatically set at "restricted mode" via our filtering system. Teacher devices and pupil devices are set up with IP addresses that use a tiered filtering provided by our ISP to minimise such events. The school views that the benefit of such a website, to further the learning of its pupils, far outweighs the potential risks.

5.1 Authorising Internet Access.

- During Early Years, Foundation and Key stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials. If children are given the opportunity to search the internet, or access websites that they are familiar with, it must be done under close supervision.
- At Key Stage 2, Internet will be accessed within a supervised environment.
- A consent form, allowing a child to access the Internet within school and accepting that the school cannot be held responsible for their child inadvertently viewing inappropriate materials, will be offered for parents to sign as a child starts our school. (*See "Parent Internet Consent Form" Appendix 1*)

- Incidents will be reported to the ICT Lead and Head of School and recorded on our Incident Logs, with incidents tagged specifically as e-safety breaches of conduct. Action to be taken will also be recorded with cases kept "open or closed" according to action taken.
- Members of staff may request the use of the school's Internet to use on their personal devices for work purpose. They agree to follow the same rules of the school policies when using their own equipment as they do when using school equipment. Access is only permissive when a secure password has been created via the ICT Lead or ICT technicians.
- All members of staff and children will be issued with a school email address, enabling them to communicate effectively on matters pertaining to school life only.
- Supply staff (short term) will use school owned devices where possible. They will not be given access to the Internet on personal equipment unless agreed with the Head of School. Long term supply cover will adhere to the same Internet access rules as permanent staff.

5.2 Managing Filtering

- The school ISP is contracted to manage and monitor Internet access to ensure systems protect pupils at all times. They liaise, report any incidents in real-time to the ICT Lead and ICT Technicians, to ensure that a dynamic security system is in place.
- Pupils will be taught what to do if they come across unsuitable on-line materials.
- If staff or pupils come across unsuitable on-line materials, the site must be reported to the technician or ICT Lead. These incidents will be deemed to be closed when the Filtering has been updated to block such content.
- Staff, pupils and parents are not permitted to use any school devices to access inappropriate materials online such as gambling websites or pornography.
- Auction sites may also not be accessed for personal use, during the school day.
- At regular intervals the ICT technician or ICT Lead will carry out checks to ensure that the filtering methods selected are appropriate, effective and of a reasonable level to ensure learning can proceed appropriately.

5.3 Social networking and personal publishing sites.

- The school will control access to social networking sites (many already blocked through the filtering system) and will educate pupils, staff and parents in their safe and appropriate use. They will educate and reinforce to children of the age appropriateness rules that such sites use.
- Information will be communicated to pupils and parents to advise of the potential dangers for primary aged pupils, including signposting to advice via newsletters or online communications.
- Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location.
- Pupils will be taught about the dangers of communicating with people they do not know.
- When teaching e-safety aspects, moderated social networking sites, appropriate to the children's age will be used.
- Pupils will be advised how to use nicknames and avatars to ensure individuals are not identifiable.
- Staff and pupils must not access social networking sites for personal use during the teaching day.

- Staff will be advised not to accept current pupils as “friends” on social networking sites.
- Staff awareness should be raised as to the possible implications of adding parents of pupils as “friends” on social networking sites, and do so at their own risk.
- Staff will be reminded of their professional position within the school community and the possible impact of their personal information being shared on these sites. Staff need to refer to their professional code of conduct. Any incident which is deemed to have broken the code may lead to disciplinary action.
- Members of staff will be encouraged to set their personal security settings to high to minimise access to all information in a digital form.
- Abuse of members of staff on social networks is not acceptable. If necessary, this will communicated to parents.
- The school will monitor and comply to GDPR’s with regards to its use of photographs used to promote school activities.

6. Managing Online Learning

Some learning environments can be used by pupils and parents both inside and outside of school to access online materials such as resources or homework.

- Pupils, staff and parents will be given log-in details for school managed resources.
- Should pupils add content, it must adhere to school protocol by being fit and appropriate for purpose.
- Personal information about pupils will not be accessible by anyone other than their own parents / guardians and members of staff. (Compliance with GDPR)
- Internet links (including videos) signposted by staff will have previously been checked for suitability.
- Rickley Park is not responsible for children’s ISP settings within their home setting. However, parents will be reminded of good practise to set these to a suitable level via home-school communications.

7. Communication Technology.

In school pupils will not communicate with members of the public via the internet unless it is for educational purposes and has been previously risk assessed by teachers.
Staff, parents and pupils are reminded that negative comments made about each other via the Internet and e-mails are not accepted by the school. Incidents of this nature will be reported to the Head of School and recorded on our Incident Logs and dealt with appropriately.

7.1 E-mail

- The school provides all staff with a Microsoft email account and children with a Gmail account, specifically managed by the School.
- Pupils and staff must immediately tell a responsible adult if they receive offensive e-mail. If the incident is considered serious it must be recorded on the Incident Logs and dealt with by the appropriate line-manager or Head of School.
- Pupils will be taught in Computing lessons, that in e-mail communication, pupils should not reveal their personal details or those of others, or arrange to meet anyone without specific permission.

- Pupils and staff will also be made aware that incoming e-mails from unknown senders should be treated as suspicious and that links that appear in e-mail should not be followed. Attachments should also not be opened unless the author is known.
- The forwarded of chain letters is not permitted using school e-mail accounts.

7.2 Instant Messaging

- Pupils are taught (through lessons on E-safety and cyberbullying) about the potential risks of engaging with others via Instant Messaging software for a variety of devices and websites such as Facebook /WhatsApp.
- Pupils are advised to only converse with people they know, however it will be emphasised that due to the nature of instant messaging they will not be able to see or know exactly who they are communicating to.
- Pupils are taught about how to respond and what to do if they receive instant messages that are offensive. This includes reporting to a responsible adult.

7.3 Managing videoconferencing and webcam use.

- Videoconferencing and webcam use will be appropriately supervised for the pupil's age and will be for educational purposes only.
- The appropriateness of people communicated with for videoconferencing should be risk-assessed by the school.

8. Use of School ICT Resources Outside School.

8.1 Staff

- Any use of mobile devices by staff and pupils to access the Internet out of school is subject to the same code of conduct as in school.
- Staff are permitted to connect school equipment to their own Internet connection but should be reminded that this access will be unfiltered.
- Virus protection that has been installed on school equipment must remain enabled when attached to ISP's other than that of the schools.
- Staff must be aware that they are ultimately responsible for any material accessed should they allow others to use their school equipment.
- Staff need to be aware that data held on individual laptops is subject to the laws of GDPR. As such, all school laptops are to be loaded with data encryption software or databases to be held within the cloud and not permanently held on such a device.

8.2 Pupils

- Pupils are encouraged to use school ICT equipment in outside areas and on school visits for educational purposes.
- The use of such equipment is governed by the rules that apply in school and monitored by staff accompanying the pupils.

9. Published Content.

The school aims to publish information to parents, as well as providing the opportunity for pupils to publish their work and achievements to the school community and sometimes to a wider audience. When such content is published, the security of staff and pupils is essential.

- Written permission from parents or carers will be obtained before digital images are published on the school website or other secure external websites and local newspapers. "Parent Internet Consent Form" (*Appendix 1*). This document is signed to give or deny permission when a child starts school.
- Class teachers are given a list for all pupils as to parents who have not given permission to have their child's photographs published on any such site. A copy of this list is held centrally within school for access by any other staff.
- Editorial responsibility for the school website is currently held by the Head of School who ensures that content is accurate and appropriate.
- Staff and pupil personal contact information will not be published. This information will be held centrally by the school office.
- Photographs that include pupils will be selected so that, whenever possible, individual pupils cannot be identified or their image misused, however it is understood that this is not always possible.
- Pupil's full names will not be used anywhere on a website, particularly in association with photographs, unless previously agreed with the pupil's parents / guardians.
- Within lessons, teachers may choose to use quality external websites (risk-assessed) for children to publish their work to, so that it reaches an audience beyond school (e.g. blogs, story-creating websites and podcast housing websites.)
- All materials published must be the author's own work or where permission to reproduce has been obtained, clearly marked with the copyright owner's name.
- All digital images obtained via the internet and used in published work will be appropriately referenced.

10. Personal Data (to be read in conjunction with the IFtL General Data Protection Policy)

- Personal data stored about staff, pupils and parents on the school network will only be accessed when needed for work purposes. Members of staff will only have access to this information in an appropriate way.
- Only necessary staff, such as the ICT Technicians have access to SIM's and other personal data that is held by the office.
- Personal data can only be accessed via secure log-on and from a managed network. This ensures that sensitive information cannot be accessed when not linked to a school network.
- "Zombie" accounts (accounts of staff who are no longer employed by the school,) are removed by the ICT Technician from when a member of staff is no longer an employee.

11. Stakeholders and the policy.

11.1 Pupils and E-safety.

- Internet safety rules will be prominently displayed around the school. They will be referred to and discussed with pupils regularly to encourage Smart Safety.
- Pupils will be informed that the network and Internet use will be monitored and any inappropriate actions followed up by a member of staff.
- E-safety training will be embedded within the Computing scheme of work and will be taught both discretely and within curriculum lessons for each year group.

11.2 Staff and the E-safety Policy.

- All staff have access to this policy on the school website.
- Staff are aware that network and Internet traffic (including emails) can be monitored and traced to an individual user if a concern about misuse is reported.
- Staff will be directed towards age appropriate resources on E-safety to further their own understanding and awareness.

11.3 Parents and the E-safety policy
Internet access in most pupil's home is now commonplace. The school aims to inform and educate parents of the potential dangers of unrestricted internet access for children in order to have a consistent approach to Internet safety.

- Parent's attention will be drawn to the School E-safety policy via school newsletters and online communications so that parents can access it at home.
- Parent / pupil E-safety guidance to signpost parents to resources they can use at home is communicated by the school.
- The school will communicate up-to date, current recommendations to ensure both parent/guardian and child remain safe when using devices both at home or within school.

11.4 The Governing Body and the E-safety Policy.
If a reported E-safety incident is deemed serious by the Head of School, it will be reported to the Governing Body, who will seek professional advice first, before contacting the person in question so they do not have a chance to delete any materials that may be needed to provide evidence.
The Governing Body take pupil safety seriously and will review the policy and its implementation and impact, on a regular basis.

12. Handling E-safety Complaints.

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- In the case of the complaint being made in relation to the Head of School, this will be referred to the Governing Body.
- Complaints of a child protection nature will be dealt with in accordance with the school Child Protection Policy (recorded Incident Logs)