John Perry Primary School



E-safety Policy

Reviewed: October 2024
Next review: October 2025

E-safety Policy

Introduction

ICT in the 21st Century is an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, we need to build in the use of these technologies in order to equip our young people with the skills to access lifelong learning and employment.

E-Safety encompasses the use of new technologies, internet and electronic communications such as mobile phones, collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

Teaching and learning

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 students 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.
- Internet use will enhance learning.
- The school's 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 Internet use.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- 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 as far as possible.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Online Safety Act (2023)

E-safety in the curriculum

ICT and online resources are increasingly used across the curriculum. We believe it is essential for e-safety guidance to be given to the pupils on a regular and meaningful basis. We continually look for new opportunities to promote e-safety.

- We provide opportunities within the ICT and PSHE curriculum areas to teach about e-safety.
- Educating pupils on the dangers of technologies that may be encountered outside school is done informally when opportunities arise and as part of the curriculum. Pupils are taught about copyright and respecting other people's information, images, etc. through discussion, modelling, and activities as part of the ICT curriculum.
- Pupils are aware of the impact of online bullying through PSHE and are taught how to seek help if they are affected by these issues. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies (cyber bullying)
- Pupils are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the ICT curriculum
- Pupils are taught about the risks inherent in using social media, particularly if they are contacted by people they do not know

Managing Internet Access

Children will have supervised access to Internet resources

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection will be updated regularly.
- Security strategies will be discussed with LBBD LEA.

- Staff must preview any recommended sites before use. Particular care must be taken when using search engines with the children as these can return undesirable links.

- If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents need to be advised to supervise any further research.

- Our internet access is controlled through the LGFL web filtering service.

- If staff or pupils discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to an ICT lead, technician or member of SLT.

- It is the responsibility of the school, by delegation to the network manager, to ensure that antivirus protection is installed and kept up-to-date on all school machines.

E-mail

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- E-mail 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.

Managing filtering

- The school will work with the LA, DFES and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover an unsuitable site, it must be reported to the e-Safety (IT Lead).
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

The school web site

John Perry Primary School values the contribution that a website / VLE (virtual learning environment) can make to the life and role of the school in a modern society. The John Perry Primary School website / VLE has 5 important roles:

1. To provide information to prospective parents and teachers, the wider community and the world
2. To act as a communication channel between teachers, parents, pupils and school management
3. To improve pupil learning
4. To raise standards in teaching and learning.

Safeguarding

The safety of children and other users who appear or are referred to on the published site and extranet is of paramount importance.

Publishing names, images and work.

- Children's names will be published as their first name only e.g. Trevor, or if required, first name and last name initial e.g. Trevor D.
- Any images of children will not be labelled with their names.
- No close-up pictures of individual children will be available online- only group photographs with two or more children (Unless parental consent has been given).
- Children will only be shown in photos where they are suitably dressed.

- Personal details of children, staff and governors, such as home addresses, telephone numbers, personal e-mail addresses, etc, will not be released via the website or school e-mail.

Privacy

- Adults have the right to refuse permission to publish their image on the published site or Intranet.
- Parents have the right to refuse permission for their child's work and/or image to be published on the published site or Intranet
- Those wishing to exercise this right should express their wishes in writing to the Headteacher, clearly stating whether they object to work, images, or both being published, to the published site or Intranet.. Parents will be notified of this right by publication of this policy on an annual basis.

Monitoring Maintenance and Editing

At least two people should have the knowledge to maintain and edit the site, and they must pass on their knowledge to a successor at the end of a term of office. Social networking and personal publishing

- The school will block/filter access to social networking sites.
- Newsgroups will be blocked unless a specific use is approved.
- 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 spaces outside school is inappropriate for primary aged pupils.

Emerging Technologies

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

Pupils are not allowed to bring mobile phones into school and if they do, the phone will be confiscated and returned at the end of the school day. Persistent offenders regarding this school rule will have their phone confiscated until a parent / guardian is able to collect it. The sending of abusive or inappropriate text messages outside of school is forbidden.

Protecting personal data

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

Policy Decisions Authorising Internet access

- The school will keep a record of all staff and pupils who are granted Internet access. The record will be kept up-to-date, for instance a member of staff may leave or a pupil’s access be withdrawn.
- At Key Stage 1, access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials.
- Parents will be asked to sign and return a consent form. Upon a non-return of the form it will be assumed that the parent has granted permission for internet use.

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 cannot accept liability for the material accessed, or any consequences of Internet access. The school will audit ICT provision 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 the Headteacher. Any complaint about staff misuse must be referred to the Headteacher who has a duty to report such incidents to the governing body.

Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

Pupils and parents will be informed of the complaints procedure.

Communications Policy

Introducing the e-safety policy to pupils

E-safety rules will be posted in all networked rooms 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 the School e-Safety Policy and its importance explained.

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

Enlisting parents' support

Parents' attention will be drawn to the School e-Safety Policy in newsletters, the school brochure and on the school Website. Reviewing the e-safety policy

The e-Safety Policy is part of whole school development and relates to other policies including those for ICT, bullying and for child protection.

Our e-Safety Policy has been written by the school, building on BECTA and government guidance. It has been agreed by senior management and approved by governors. The e-Safety Policy and its implementation will be reviewed annually.

The e-Safety Policy was revised by the IT Lead/ Deputy Safeguarding Lead Appendix 1

John Perry Primary School Pupil e-Safety Agreement

This is to be read through with your parent(s).

At John Perry Primary School, we believe that accessing the internet is of great educational benefit, however we expect all pupils to be responsible for their own behaviour on the Internet, just as they are anywhere else in school. This includes materials they choose to access, and language they use.

- Pupils using the World Wide Web are expected not to deliberately seek out: offensive materials. Should any pupils encounter any such material accidentally, they are expected to report it immediately to a teacher.

- Pupils are expected not to use any rude language in their email communications and contact only people the teacher has approved. It is forbidden to be involved in sending chain letters.
- Pupils must ask permission before accessing the Internet.
- Pupils should not access other people's files unless permission has been given.
- Computers should only be used for schoolwork and homework unless permission has been granted otherwise.
- No program files may be downloaded to the computer from the Internet.
- No programs on disc or CD Rom should be brought in from home for use in School.
- Personal printing is not allowed on our network for cost reasons (e.g. pictures of pop groups/cartoon characters).
- No personal information such as phone numbers and addresses should be given out and no arrangements to meet someone made.
- Pupils consistently choosing not to comply with these expectations will be warned and subsequently, may be denied access to Internet resources.

Appendix 2

At Home

As a parent you'll know how important the internet is to children – they use it to learn, play, socialise and express themselves. It's a highly creative place of amazing opportunities. But the technology children use every day can seem a bit daunting and you might worry about the risks your child can face online – such as bullying, contact from strangers or the possibility of them seeing illegal or inappropriate content.

You can download a simple checklist here that may help you start to protect your children online and decrease the risks they face. Or you can engage with your children regarding their use of the internet while at home. Here are some conversation starter ideas from www.childnet.com

- Ask your children to tell you about the sites they like to visit and what they enjoy doing online.
- Ask them about how they stay safe online. What tips do they have for you, and where did they learn them? What is OK and not OK to share?
- Ask them if they know where to go for help, where to find the safety advice, privacy settings and how to report or block on the services they use.
- Encourage them to help. Perhaps they can show you how to do something better online or they might have a friend who would benefit from their help and support.
- Think about how you use the internet as a family. What could you do to get more out of the internet together and further enjoy your lives online

John Perry Primary School letter to parents/carers reporting an online safety concern.

When a child is involved in an online safety concern, whether they are the victim or perpetrator, a letter will be sent home to the parent/carer of the child to inform them of the incident.

There will also be a log of these incidents kept in a file for the Safeguarding Team and SLT to monitor.

John Perry Primary School
Charles Road
Dagenham
Essex
RM10 8UR
Tel: 020 8270 4622
Email: office@johnperry.bardaglea.org.uk
Head Teacher: Mr W Pedro

02.10.2024

Dear Parents and Carers,

An online incident has been reported to the safeguarding team.

This involved _____ (e.g. the sharing of a link to an inappropriate video to a group of our pupils).

If your child is allowed access to the internet and social media at home, we urge you to be vigilant in monitoring its use and be reminded of the age restrictions for opening accounts on social media platforms.

Also, to ensure that your child is fully aware of the people they are in contact with.

If you have any concerns about your child's group of contacts, delete and block the numbers and consider changing your child's mobile number.

If you believe your child is being targeted by anyone online, call the police on 101.

Thank you for your support in this matter. Working together, we can ensure that our children feel safe and protected at all times.

Please contact the school if you have any concerns.

Yours sincerely,

Safeguarding Team