CAVERSHAM PARK PRIMARY SCHOOL

E-Safety Policy

Our e-safety policy has been written using government guidance.

Contents

Teaching and Learning

1.1 Why internet use is important

- The internet is an essential element of the 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.
- The internet is part of the statutory curriculum and a necessary tool for staff and pupils.
- Pupils use the internet widely outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

1.2 Internet use will enhance learning

- The school internet access is designed expressively for pupil use and includes filtering appropriate to the age of the children.
- Staff will guide pupils in on-line activities that will support their learning outcomes planned for the pupil's age and maturity.
- Pupils will be taught about acceptable use of the internet through the school's e-safety curriculum.
- Pupils will be educated in the effective use of the internet in research, including the skills of knowledge of location, retrieval and evaluation as part of the school's computing curriculum.

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 will be taught to be critically aware of the materials they read and be shown how to validate information before accepting its accuracy.
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using the internet material in their own work.

Managing Internet Access

2.1 Information System Security

- The school computer system's security will be reviewed regularly under the guidance of the Computing Subject Leader and the technical support service.
- Virus protection will be updated regularly on all school devices.
- Portable media must not be used by children without specific permission and followed by a security check.
- The Computing Subject Leader /technical support service will review the system capacity regularly.

2.2 E-Mail

- The personal e-mail addresses of staff and governors should not be used for school purposes.
- Access to school e-mail is at the discretion of the school and can be terminated at any time.
- Pupils are taught how to use email responsibly and how to report inappropriate/offensive content.
- E-mail sent to an external organisation should be carefully written and authorised before sending, in the same way as a letter written on school headed paper.
- Personal information about pupils must not be shared externally via email.
- Any pupils or staff using offensive or bullying language or behaviour through e-mail will have their account terminated.

2.3 Published Content on the School Website

- The contact details on the website should be the school address, e-mail and telephone number. Staff or pupil personal information will not be published.
- The headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

2.4 Publishing Pupil's Images and Work

- Photographs that include images of pupils will be selected carefully and only with parental permission.

- Pupils' names will not be used anywhere on the website, particularly in association with photographs, unless consent has been granted.
- Written permission from parents / carers will be obtained before the photographs of pupils are published on the school website. It is not possible to download or save photographs from the website.
- Pupils' work can only be published with the permission of the pupil and parents/carers.
- Access to the Foundation Stage Online Learning Journey is password protected. Parents / carers will be unable to download or save images from the resources and can only access information related to their child.

2.5 Social Networking and Personal Publishing

- The school will block access to social networking sites.
- 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 will be advised that the use of social network spaces designed for children over the age of 13 outside school is inappropriate for primary age pupils.

2.6 Managing Filtering

- The school will work with the technical support company and 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 co-ordinator or Computing Subject Leader so that it can be reported and blocked. A log of incidents is kept by the Computing Subject Leader.
- Children must be taught about safe searching before being allowed to search online in school.
- Child friendly search engines are to be used whenever possible.
- Staff should not perform a search on a search engine (e.g. Google search) in view of the children without doing so prior to the lesson (in school) to check what results are drawn up.
- Teachers should ensure that children are not left to search the internet unsupervised and should check the sites that they plan to use with children prior to the activity.
- Children should not be left unsupervised at anytime whilst using the internet.

2.7 Managing the Emerging Technologies

- Emerging technologies will be examined for educational benefit and risks before use in school is allowed.
- Mobile phones will not be used during lessons. Pupils are not allowed to bring mobile phones in to school unless permission is granted from the Headteacher. They need to be handed into the school office, where they will then be locked away during the school day. The sending of abusive or inappropriate messages is forbidden.
- Staff will use the school phone where contact with pupils' parents/carers is required.
- Pupils are taught how to report cyber bullying and offensive content.

2.8 Protecting Personal Data

- The use by staff and monitoring by the School of its electronic communications systems is likely to involve the processing of personal data and is therefore regulated by the General Data Protection Regulation (GDPR) and all data protection laws and guidance in force.
- The General Data Protection Regulation (GDPR) aims to protect the rights of individuals about whom data is obtained, stored, processed or supplied and requires that organisations take appropriate security measures against unauthorised access, alteration, disclosure or destruction of personal data.

Policy Decisions

3.1 Authorising Internet Access

- All staff must read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource.
- The school will keep a record of all staff or pupils who are granted internet access. The record will be kept up-to-date: for instance, if a member of staff leaves or a pupil's access is withdrawn.
- Parents/carers will be informed that pupils will be provided with supervised internet access.

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 the internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school will not accept liability for the material accessed, or any consequences of internet access.
- The school will audit computing provision to establish if the e-safety policy is adequate and that the implementation is effective.
- The use of the computer systems without permission and for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.

3.3 Handling E-safety Complaints

- Complaints of internet misuse will be dealt with by a member of the senior leadership team.
- Any complaint about misuse must be referred to the Headteacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents/carers will be informed of the complaints procedure.

3.4 Community use of Internet

- The school will liaise with local organisations to establish a common approach to e-safety.
- The school will be sensitive to internet related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice, however they cannot be held responsible.

Communications Policy

4.1.1 Introducing the E-Safety Policy to Pupils

- E-safety rules will be posted in all networked rooms and discussed with pupils regularly throughout the school year.
- Pupils will be informed that network and internet use will be monitored.
- Instruction in responsible and safe use should precede internet access.
- The school has its own internet safety curriculum to educate children about e-safety as part of the computing curriculum covering both school and home..
- The CEOP, Becta and UK Safer Internet Centre e -safety resources will be used to support this curriculum.
- The school takes part in "Internet Safety Day" each year, during which age appropriate assemblies and lessons are carried out and pupils are taught about being safe online;

4.2 Staff and the E-Safety Policy

- All staff will be given the school E-Safety Policy and its importance will be explained.
- Staff should be aware that internet traffic can be monitored and traced to the individual user. Discretion and personal conduct is essential.

4.3 Enlisting Parents'/Carers' Support

- Parents'/carers' attention will be drawn to the school E-Safety Policy in newsletters and on the school website.
- E-safety information sessions are held to inform parents about the benefits and dangers of the internet and give them practical advice on how to protect their children.

Policy Date	Review Date
May 2019	December 2022