PRINCES PRIMARY SCHOOL

E-SAFETY POLICY

May 2016

This Policy has been informed by the local and government guidance.

- This policy applies to all members of the school community (including staff, pupils, volunteers, parents / carers and visitors) who have access to and are users of ICT systems in school. All staff are provided with the School Internet Policy. All staff must accept the terms of the 'Responsible Internet Use' statement before using any Internet resource in school.
- The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information and business administration systems.
- Where appropriate, e-safety messages are reinforced as part of the curriculum**,** pupils are taught what is not acceptable and are given clear objectives for Internet use.
- Internet access is planned to enrich and extend learning activities. Staff guide pupils in online activities that will support the planned learning outcomes.
- The school Internet access is designed expressly for pupil use and includes appropriate filtering Access to the Internet is by adult demonstration with occasional directly supervised access to specific, approved on-line materials. The school takes all reasonable precautions to ensure that users only access appropriate material; pupils are guided to sites checked as suitable for their use. Where pupils are allowed to freely search the internet, e.g. using search engines, staff should be vigilant in monitoring the content of the websites the young people visit
- Any suspected misuse or problems should be reported. Responsibility for handling incidents will be delegated to a senior member of staff.
- Pupils may only use approved e-mail accounts on the school system
- Pupils are not allowed access to public or unregulated chat rooms.
- The school is responsible for ensuring that the school infrastructure is as safe and secure as is reasonably possible. The school works in partnership with the LA, DFE and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
- The server is located securely and physical access restricted
- All users have clearly defined access rights to school ICT systems and iPads
- Virus protection for the whole network is installed and current. The school ICT systems will be reviewed regularly with regard to security
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990. Methods to identify, assess and minimise risks will be reviewed regularly.
- Any complaint about staff misuse must be referred to the head teacher. There may be occasions when the police must be contacted. Early contact could be made to establish the legal position and discuss strategies.
- Materials derived from the internet should comply with copyright law

PRINCES PRIMARY SCHOOL

RESPONSIBLE INTERNET USE

Rules for Staff and Students

May 2016

The school computer system provides Internet access to students and staff. This Responsible Internet Use statement will help protect students, staff and the school by clearly stating what is acceptable and what is not.

- Access must only be made via the user's authorised account and password, which must not be given to any other person.
- Staff and pupils are not permitted to use their own software on the school computer systems. This is to ensure that viruses are not introduced into the school systems by this method
- School computer and Internet use must be appropriate to the student's education or to staff professional activity.
- Copyright and intellectual property rights must be respected.
- In accordance with the Data Protection Act users must use their school email address and not their personal address for school related matters.
- In accordance with the Data Protection Act, laptops, personal computers, iPads, pen drives and other storage devices should be password protected or encrypted if personal data is to be stored on them.
- Users are responsible for e-mail they send and for contacts made.
- E-mail should be written carefully and politely. As messages may be forwarded, e-mail is best regarded as public property.
- Anonymous messages and chain letters must not be sent.
- The use of public chat rooms is not allowed
- It is against school policy for staff to accept parents as friends on social networks.
- The school ICT systems may not be used for private purposes, unless the head teacher has given permission for that use.
- Use for personal financial gain, gambling, political purposes or advertising is forbidden.
- The security of ICT systems must not be compromised, whether owned by the school or by other organisations or individuals.
- Irresponsible use may result in the loss of Internet access.
- The school may exercise its right by electronic means to monitor the use of the school's computer systems, including the monitoring of web-sites, the interception of E-mails and the deletion of inappropriate materials in circumstances where it believes unauthorised use of the school's computer system is or may be taking place, or the system is or may be being used for criminal purposes or for storing text or imagery which is unauthorised or unlawful.