WOOTTON PARK

'Ipsum quod faciendum est diutius'

Title	**E-Safety Policy**
Year	2017/2018
Author	Dan Rosser
Governor Link	Andre Gonzalez De Savage
Date approved by Full Governing Body	September 2018
Review Date	September 2019

E-Safety Policy Introduction

This E-Safety Policy is part of the approach we take to safeguarding the well-being of learners. This E-Safety Policy has been written by the school, building on government guidance.

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 learners with high 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 learners in their daily working lives at school.

Internet use will enhance learning

The school Internet access is designed expressly for learner use and includes filtering appropriate to the age of learners. Learners will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use. Learners will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

Learners will be taught how to evaluate Internet content

The school will ensure that the use of Internet derived materials by staff and learners complies with copyright law. Learners will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Core Principles

The school must comply with a variety of legislation in this regard, including:

i. The Data Protection Act 1998;

ii. The Human Rights Act 1998;

iii. The Computer Misuse Act 1990;

iv. The Regulation of Investigatory Powers Act 2000;

v. The Freedom of information Act 2000;

vi. The Copyright, Designs and Patents Act 1988;

vii. The Electronic Communications Act 2000; together with various Statutory Instruments and other pieces of legislation.

Notwithstanding the requirements of the Data Protection Act, the school retains its right to monitor the use of its systems by any user in order to protect its legitimate business and reputation.

Information system security

School ICT systems capacity and security will be reviewed annually. Virus protection is updated on an ongoing basis. Use of the internet will be monitored to ensure appropriate use by all members of the school community. Anyone acting inappropriately will be removed from the system.

E-mail

Learners may only use approved e-mail accounts on the school system. Learners must immediately tell a teacher if they receive offensive e-mail or pop-ups. Learners must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone following unauthorised communications.

E-mail sent to an external organisation should be written carefully and authorised by a teacher before sending, in the same way as a letter written on school headed paper. The forwarding of chain letters is not permitted.

Published content and the school web site

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

A designated member of staff will have responsibility for the system and will ensure that content is accurate and appropriate.

Publishing learner's images and work

Learners' full names will not be used anywhere on the website, particularly in association with photographs.

Written permission from parents or carers will be obtained before photographs of learners are published on the school website. Learners' work can only be published with the permission of the learner and their parents.

Social networking and personal publishing

The school will block/filter access to social networking sites other than pre-approved educational sites. Newsgroups will be blocked unless a specific use is pre-approved. Learners will be advised never to give out personal details of any kind that may identify them or their location. Learners and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged learners. Secondary and post-16 learners will be guided on use.

Managing filtering

The school will work with ICT providers, the DfE and the Internet Service Provider to ensure systems to protect learners are reviewed and improved. If staff or learners discover an unsuitable site is accessible, it must be reported immediately to the Network Manager. Senior leaders will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Managing videoconferencing

Learners will be required to gain permission from the supervising teacher before making or answering a videoconference call. Videoconferencing will be appropriately supervised for the learners' age.

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 unless for a pre-approved educational purpose. The sending of abusive or inappropriate text messages is forbidden.

Protecting personal data

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

Authorising Internet access

The school will keep a record of all staff and learners who are granted Internet access. The record will be kept up-to-date, for instance, a member of staff may leave or a learner's access be withdrawn. For EYFS/ 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. For KS2/3/4/5 learner access, under age-appropriate supervision, is allowed.

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 will not 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 a senior member of staff in line with the WPS Complaints Policy. Complaints of a child protection nature must be dealt with in accordance with school child protection procedures and reported to the Designated Safeguarding Lead. Learners and parents will be informed of the complaints procedure via the School website.

Where required and in accordance with the Law, issues around e-safety that are potentially illegal will be reported to the Police.

Introducing the e-safety policy to learners

E-safety rules will be posted in all networked rooms and discussed with the learners at the start of each year. Learners 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 therefore essential. Any staff in breach of the acceptable use agreement or the e-safety policy will be referred through the disciplinary policy.

Enlisting parents' support

Parents' attention will be drawn to the School e-Safety Policy in newsletters, the school brochure and on the school Web site. Parents should also be aware of their own conduct when using modern technologies and pay reference to the policy on use of social media.

Review

The E-Safety Policy and its implementation will be reviewed annually by Governors.

This policy is to be read in conjunction with the Safeguarding and Promoting Welfare Policy, the Anti-Bullying Policy and the Behaviour Policy.