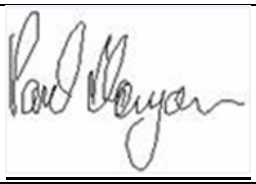
Whitehall Park School

LEARN ENJOY SUCCEED

E-Safety Policy

This policy applies to all children in the school including EYFS

Signed:	
Chair of Governors:	Paul Domjan
Approved:	23rd March 2017
Review Date:	October 2019

Whitehall Park School
LEARN ENJOY SUCCEED

CONTENTS

1.0 Rationale

This E-Safety Policy is part of the approach we take to safeguarding the well-being of pupils.

This E-Safety Policy has been written by the school, building on government guidance.

2.0 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 pupils 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 pupils in their daily working lives at school.

3.0 Internet use to enhance learning

Internet access at school is designed expressly for pupil use and includes 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.

4.0 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 shown how to validate information before accepting its accuracy.

5.0 Information system security

School ICT systems capacity and security will be reviewed annually.
Virus protection is updated on an ongoing basis.
Advice on security strategies will be monitored on the School's ICT web page and clarification sought as necessary.

6.0 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 or pop-ups.
Pupils 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.

7.0 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 pupils' personal information will not be published.

The Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

8.0 Publishing pupils' images and work

Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified if permission has not been given.

Pupils' 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 pupils are published on the school website.

Pupils's work can only be published with the permission of the pupil and their parents.

9.0 Social networking and personal publishing

The school uses LGfL as internet providers who 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. Pupils will be advised never to give out personal details of any kind that 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 children.

10.0 Managing filtering

The school will work with the DfE and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.

If staff or pupils discover an unsuitable site is accessible, it must be reported to the E-Safety Coordinator.

SLT will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable. For staff use, filtering will be tuneable.

11.0 Managing videoconferencing

Pupils will be required to gain permission from the supervising teacher before making or answering a videoconference call.

Videoconferencing will be appropriately supervised for the pupils' age.

12.0 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 at any time.

13.0 Protecting personal data

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

14.0 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.

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 pupil access, under age-appropriate supervision, is allowed.

15.0 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. Neither the school nor BPET can 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.

16.0 Handling e-safety complaints

Complaints of Internet misuse will be dealt with by a senior member of staff.

Any complaint about staff misuse must be referred to the head teacher.

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.

Discussions will be held with the Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues

17.0 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.

18.0 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.

19.0 Enlisting parents' support

Parents' attention will be drawn to the School e-Safety Policy in newsletters and on the school website.

20.0 Monitoring and Evaluation

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

21.0 Approval by Local Governing Body and Review Date

This policy has been formally approved and adopted by the Local Governing Body at a formally convened meeting.

Signed: _____

(Chair of Governing Body)

Date: _____

Review date: _____

End of statement