Westfield Primary Academy

Internet Safety Policy

Date Approved	**14th July 2015**
Signed	(Chair of School Improvement Committee)
Minuted	**14th July 2015** (Date)
Date of Next Review	**July 2016**

1. Introduction

1.1 The school will appoint a designate Internet Safety lead.
1.2 Our Internet Safety Policy has been written by the school, building on the recommendations of other schools and government guidance. It has been agreed by the senior management and approved by governors.
1.3 The Internet Safety policy will be reviewed annually.

2. How will we use the Internet safely to Enhance Learning

2.1 The school Internet access will be designed expressly for pupils use and will include filtering appropriate to the needs of the curriculum.
2.2 Pupils will be taught what acceptable internet use is and what is not, with clear objectives.
2.3 Internet access will be planned to enrich and extend learning activities. Access levels for each key stage will be reviewed to reflect the curriculum.
2.4 Staff should guide pupils in on-line activities that will support the learning outcomes planned.
2.5 Pupils will be educated in the effective use of the internet in researching, including the skills of: selecting, retrieving, collecting, analysing and storing information.
2.6 The school will endeavour to ensure that the copyright law is complied with by staff and pupils.

3. Maintenance of Information Systems

3.1 The security of the school information systems will be reviewed regularly by the ICT technician.
3.2 Virus and Spyware protection will be installed and updated regularly by the ICT technician.
3.3 The ICT technician will review system capacities regularly and update the relevant person/s.

4. The Management of E-mails

4.1 Users may only use approved e-mail accounts.
4.2 Emails sent from a school email address to external organisations should be written carefully, in the same way as a letter written on school headed paper would be.
4.3 Email subscriptions using the school email address to websites and other electronic services should be for school and curriculum use only.

4.4 Authorisation is required when publishing, sharing or distributing any personal information about pupils and staff (such as, photographs, home address, e-mail address, telephone no. etc)

5. Publication of Pupils Images and Work

5.1 Pupils full names will not be used anywhere on the website or open blog.
5.2 Photographs will only be published on the school website and the e-learning platform (and only with the permission of the parent/carer).

6. Management of Social Networking

6.1 The school will have the option to block/filter access to social networking sites.
6.2 Pupils and staff will be advised never to give out personal details of any kind which may identify themselves, others or locations.
6.3 The school should be aware of and deal with bullying that can take place through social networking.
6.4 The school Facebook page (and other social media pages which may consequently be set up) will be maintained by the Head of School and any other person authorised by the Head of School.

7. Management of Filtering

7.1 The school will work with the ICT technician to ensure that systems to protect pupils are reviewed and improved.
7.2 If staff or pupils discover unsuitable sites this must be reported to the Internet Safety co-ordinator who will then take relevant action.
7.3 Regular checks will be carried out by the ICT technician who will inform senior members of staff or the Computing co-ordinator of appropriate filtering methods.
7.4 Any material that the school believes is illegal must be reported to appropriate agencies eg. Child Exploitation and Online Protection Centre (CEOP).

8. Protection of Personal Data

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

9. Management of Data Storage

9.1 All members of staff can use a memory stick for the transfer of documents, records and photographs.
9.2 All data must be transferred as soon as possible from memory sticks on to school computers. Data on memory sticks must then be deleted.
9.3 Any data on memory sticks taken outside the school building must be encrypted.

10 Community use of the Internet in School

10.1 Community users coming into school must adhere to the schools Internet Safety policy and acceptable use policy.

11. Integration of Internet Safety Policy

11.1 All children will be made aware of Internet Safety rules and these will be posted in areas with internet access. Users will be informed that network and internet use will be monitored.

11.2 All staff, pupils and parents will have to adhere to the schools Internet Safety policy and agreement, along with the acceptable use policy.

11.3 All staff and governors will be aware of the Internet Safety policy and its application and importance explained.

11.4 Staff training will be provided on Internet Safety at appropriate regular intervals.

12. Monitoring and Review

12.1 There will be an annual review of this policy by the Internet Safety and Computing co-ordinator. The updated policy will then be reviewed by the SLT, governing body and all members of staff.