BUSY BEES AND THE AFTER SCHOOL ACTIVITIES SAFE INTERNET USAGE AND E-SAFETY POLICY

OVERVIEW

Busy Bees and the after school activities has made significant investment in information technology and computer systems. Access to the internet carries with it the danger that children could find and view material that is unsuitable for them or that they could be put at risk from cyber bullying, unwanted and inappropriate contacts. This policy seeks to ensure that the internet and other forms of information communications technology is used appropriately but with safeguards to protect children from harm.

INTENT

1. To ensure that children access to inappropriate sites and locations is restricted.
2. To ensure that the use of the internet is for proper purposes set out during Busy Bees and the after school activities session
3. To protect children from harm and upset that could be caused through giving them access to inappropriate sites, materials, images and contacts.
4. To make children aware that there are inappropriate sites that are harmful and so must be avoided in school and at home.
5. To encourage children to report immediately any inappropriate, sites, materials or contacts that they find on the internet either at school or at home.
6. To ensure that children do not suffer from abuse by other children, including abuse by sexting
7. To ensure that the Busy Bees and the after school activities complies with section 127 of the communications Act 2003 and the recommendations of the Byron Report 2008.
8. To ensure the Data Protection Act 2018 is adhered to, controlling how personal information is used by the Busy Bees, the after school activities and school.
9. To ensure the Electricity at Work Regulation Act of 1989 is adhered to.

IMPLEMENTATION

1. As some mobile communication devices and mobile phones now have internet access, children bringing any mobile device into Busy Bees and the after school activities will be required to have it switched off at all times.
2. Appropriate Firewalls will be put in place and must be enabled at all times on all the computers.
3. Staff must always check that Firewalls are in place before children are allowed to access the internet.
4. Staff must not disable or bypass Firewalls on any school owned computer under any circumstances or at any time.
5. Children must be supervised by adults at all time that they are given access to the internet.
6. Staff must only use computers for work purposes. Computers used by staff either at home or in work must not be modified or used for personal use.
7. If children bring digitally stored information on disk or on pen drive or by other means, staff must check the suitability of the information before it is played on school computers.
8. Children must be encouraged to notify staff if they at any time come across unsuitable material on a computer or if they feel threatened or harassed by any form of cyber bullying.
9. Staff must notify the headteacher immediately if they find unsuitable or inappropriate material on a computer, mobile phone or storage device or if they find that a child is the subject of cyber bullying.
10. Spot checks and audits will be carried out from time to time to ensure that computers are being used appropriately.
11. Children found with mobile devices switched on in Busy Bees and the after school activities will have those devices confiscated until parents can come them pick up their child. The device will subsequently be banned from Busy Bees and the after school activities.
12. Incidents of inappropriate use of ICT or of cyber bullying will be reported to the headteacher and records will be kept.
13. The school ensures sufficient removal of personalised data, confidential data or any other data coming within the remit of the Data Protection Act from the disc or memory of the PC/item of ICT equipment. This also includes deletion of data from any other computer media disposed with the PC/item of ICT equipment (e.g. pen drive) – this is carried out by PRM Green Technologies

(PRM Green Technologies Ltd - Unit 16A Watling Street Business Park, Cannock, Staffordshire, WS11 9XG)- an approved certificate of documentation is received on disposal.

14. The school server has the software VEEM uploaded. This ensures data is backed up and saved offsite. It is also encrypted. 'Fortigate' (Router) is used as a web filtering software and blocks unauthorised websites. The Computing Lead receives a weekly e-mail with a report of blocked sites attempting to be accessed.
15. School emails are filtered using 'Barracuda'.
16. Electrical equipment is tested at regular intervals to ensure safety of use before transfer of equipment. After transfer of equipment it will be the responsibility of the new owner to comply with The Electricity at Work Regulations.

IMPACT

Children and staff will be able to enjoy and use of ICT to enhance Busy Bees and the after school activities and to access useful materials, without risk of harm or upset.

Reviewed by A. Parker Oct 24
Approved by Governing Board
Policy to be reviewed Oct 25