Windmill Hill Primary School

Online Safety Policy

OVERVIEW

Windmill Hill Primary School has made significant investment in information technology and computer systems to support teaching and learning and to give learners the opportunity to seek information and carry out research. Access to the internet carries with it the danger that learners 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 are used appropriately for learning but with safeguards to protect learners from harm.

OBJECTIVES

1. To ensure that learners access to inappropriate sites and locations is restricted.
2. To ensure that the use of the internet is for proper purposes related to the teaching, learning and curriculum of this school.
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 learners aware that there are inappropriate sites that are harmful and so must be avoided in school and at home.
5. To encourage learners 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 the school complies with section 127 of the communications Act 2003 and the recommendations of the Byron Report 2008.
7. To ensure that the school complies with 'Keeping Children Safe 2016'.
8. To follow the advice contained within the new statutory guidance on the legal duty set out in the 'Prevent Duty Guidance: For England and Wales (2015)' in conjunction with the other duties which we already have for keeping pupils safe.

STRATEGIES

1. As some mobile communication devices and cell phones now have internet access, learners bringing any mobile device into school will be required to have it switched off at all times on school premises.
2. Appropriate Firewalls will be put in place and must be enabled at all times on all the school computers.
3. Staff must always check that Firewalls are in place before learners 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. Learners must be supervised by adults at any time that they are given access to the internet.
6. If learners bring digitally stored information into school 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.
7. Learners 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.
8. Staff must notify the headteacher immediately if they find unsuitable or inappropriate material on a computer or storage device or if they find that a learner is the subject of cyber bullying.
9. Spot checks and audits will be carried out from time to time to ensure that computers are being used appropriately.
10. Learners found with mobile devices switched on in school will have those devices confiscated until parents can come into school and collect them. The device will subsequently be banned from school.
11. Incidents of inappropriate use of ICT or of cyber bullying will be reported to the headteacher and records will be kept.

12. Staff members are alert to recognise signs that pupils are in danger of being radicalised and drawn into extremism when using the internet.

OUTCOMES

Learners and staff will be able to enjoy and use of ICT to enhance teaching, learning and the curriculum and to access useful educational information and materials, without risk of harm or upset.

Revised and adopted by the Governing Body:

Date: September 2016