

Inspire, Enjoy, Achieve

E-Safety Policy

February 2016

Reviewed March 21

Chair of Governors……………………………………………………………..

Headteacher…………………………………………………………………..…..

Date……………………………………………………………………………………….

Review March 24

Cotton End Forest School

E-Safety Policy

**STATEMENT OF DEFINITION**

Cotton End Forest School sees the area of E-Safety as a child protection issue and not one that is solely evident in ICT. All staff and pupils have a duty to be aware of their own and others E-Safety at all times. This policy should be read in conjunction with the acceptable usage policy and in line with the flowchart for recording and reporting E-Safety incidents. E-Safety is not limited to school premises, school equipment or the school day, neither is it limited to equipment owned by the school. Any incident that happens during the school day will be reported in line with the flowchart for recording and reporting E-Safety incidents. Incidents from outside school that are disclosed or observed by staff will be dealt with in line with child protection procedures.

**STATEMENT OF DUTY OF CARE**

The Headteacher will have overall responsibility for all e-safety matters and will be informed of all incidents in line with the flowchart for recording and reporting e-safety incidents. This said all staff have a responsibility to support E-Safety practices in schools. Pupils and staff at all levels need to understand their responsibilities and liabilities in the event of deliberate attempts to breach E-Safety protocols or those laid out in the Acceptable Use Policy.

**SCOPE OF POLICY**

E-safety concerns the day to day running of the physical network and information passing through it whether connected via the internet, virtual private networks, intranets or local area networks. Pupils are to be taught safe practices and that the E-Safety Policy will be monitored and enforced. The school will respond to E-Safety incidents involving members of the school (staff or pupils) as if they occurred during the school day, on the school site even if perpetrated using equipment not owned or operated by the school.

**TEACHING SAFE PRACTICES**

All staff are trained in good E-Safety practices through the schools professional development activities including those given by internal and external trainers. Governors will have an overview of E-Safety practice as an agenda item on an annual basis and will be updated as the policy is revised.

Pupils are taught the nationally produced Purple Mash and Switched on Computing from Reception through to Year 6 . Whole school assemblies are also used to remind children of e-safety.

**STATEMENT OF PROVISION OF SAFE ENVIRONMENT IN SCHOOLS**

**(INCLUDING MONITORING OF THE POLICY)**

The school currently provides access to the internet through Schools Broadband as a filtered internet service provider. The school ensures that all hardware owned by the school network is provided with sufficient anti virus and firewall protection.

It is expected that all staff and pupils adhere to this policy at all times, it should be read in conjunction with the Acceptable Use Policy. The policy is monitored by both the ICT Co-ordinator and the Headteacher through the use of regular review with members of the school and in line with the flow chart for E-Safety incidents.

**PROCEDURES TO BE FOLLOWED IN THE EVENT OF A BREACH OF E-SAFETY**

All instances of E-Safety, whether by direct observation or disclosure will be taken seriously. The process to follow should an observation or disclosure be made is laid out clearly in the flow chart for e-safety incidents (Appendix 2). The flow chart should be followed and incident report completed at the earliest opportunity and in any case within 24 hours. The incident flow chart for E-Safety incidents includes the protection of evidence should there be a serious breach of E-Safety. Serious is defined as any breach that is intentional, whether by a member of the school or aimed towards a member of the school. Any device that has been involved in a serious breach should be taken, if safe to do so, and placed within the locked server room for investigation.

All breaches whether serious or not will be recorded in line with the flow chart for E-Safety incidents. The E-Safety incident log is kept in the Headteacher’s office (Appendix 3). E-Safety incidents that are deemed as serious could be incidents of sexual or violent imagery, bullying, racist or offensive text, physical attack, e-attack or sexual grooming. In these cases the E-Safety policy should be read with other appropriate policies such as Child Protection, Acceptable Use and Disciplinary. This may involve other agencies including police, social services and LSCB.

**STAFF USE OF TEACHER LAPTOPS AND SCHOOL PROPERTY**

It is expected that staff laptops and all other school-provided laptops will only be used by the employee of the school. It is important that staff take reasonable care of the school property particularly when taking school- provided equipment off-site. Staff should ensure that equipment is stored in secure locations away from public access.

**THE PHYSICAL ENVIRONMENT:**

**WIRELESS NETWORKS**

The school uses wireless networking which is encrypted to WPA 2 standard.

**PASSWORD POLICY**

All network users agree that they will not attempt to access the school network using any other

username/password than their own. This is in line with the Acceptable Use Policy.

**DATA TRANSFER**

Only sensitive data that is essential for staff to work on at home should be taken off site. Class lists with tracking data may be taken off site, however pupil information taken from SIMS including home addresses, medical, educational and personal information should not be taken off site unless pre-arranged and agreed with the Headteacher and only then should be removed in exceptional circumstances.

Any data that is removed from the school site should be removed on a school laptop with the normal level of E- Safety security as outlined in this policy or on a hardware encrypted memory stick provided by the school. These are the only methods that sensitive data should be transferred.

Information regarding staff and pupils that needs to be shared between job-share staff and between staff and Headteacher should be placed on the school network where usual data protection and E-Safety measures are in effect.

All staff have a duty to ensure that non school staff do not have access to school data being used at home as outlined in the Acceptable Use policy.

**STAFF BRINGING IN FILES FROM HOME FOR TEACHING AND LEARNING**

Any member of staff that brings files from home for Teaching and Learning is responsible for ensuring that the file they propose to use in school is free from virus/spyware/malware and it is their responsibility to ensure that the material contained in the file is fit for purpose and does not contain any offensive or copyright material.

**MONITORING AND REPORTING PROCEDURES**

Records of all incidents involving e-safety will be compiled on the standard incident report forms which are kept in the E-Safety incident report folder within the Headteacher’s office. These records may be shared with legitimate agencies as necessary to ensure E-Safety.

**FURTHER ADVICE AND GUIDANCE**

Monitoring and reporting advice from Becta:

<http://schools.becta.org.uk/index.php?section=is&catcode=ss_to_es_pp_aup_03&rid=12002>

E-safety charter: <https://selfreview.becta.org.uk/>

Becta Next generation Learning page: <http://www.nextgenerationlearning.org.uk/>

Next Generation Learning Charter: <https://selfreview.becta.org.uk/about_next_generation_learning_charter>

The Byron Report: <http://www.dcsf.gov.uk/byronreview/pdfs/Final%20Report%20Bookmarked.pdf>

The Byron Report. Children’s Summary:

<http://www.dcsf.gov.uk/byronreview/pdfs/A%20Summary%20for%20Children%20and%20Young%20People%20FINAL.pdf>

The Byron Report Executive Summary: <http://www.dcsf.gov.uk/byronreview/pdfs/Executive%20summary.pdf>

A**PPENDIX 1**

**E-SAFETY FOR PARENTS**

While it is good practice to offer parents advice on E-Safety, it is not practicable for school to offer technical advice on individual operating systems, hardware or software. The advice offered to parents should cover the main concerns regarding E-Safety and should direct them where to gain specific advice for their systems. Should any parent ask a member of staff for advice they should be given the following information.

During a period of remote learning the school may provide extra technological support where possible, under the guidance of partnership and agreed with the Headteacher. This is offered to allow a child access to education.

We should not offer advice on type of equipment or operating system other than in the most general of terms. Parents need to make their own informed choices, but will sometimes want advice from schools. There is a need to remain objective and not to favour any particular manufacturer over another. Using the internet is great for young people’s education and development. It opens up exciting new opportunities for learning. Whatever they’re up to – researching a school project, chatting with friends or playing a game – your children are likely to spend even more time surfing the web as they get older. Fortunately there are some

simple things you can do to help them surf safely and feel confident about learning online.

**FUTHER GUIDANCE**

Becta Next generation Learning page: <http://www.nextgenerationlearning.org.uk/>

Becta e-safety quiz for parents: <http://www.nextgenerationlearning.org.uk/en/Benefits/E-Safety-Quiz/>

 <http://www.nextgenerationlearning.org.uk/en/Benefits/learn-safelyonline/>

 <http://www.thinkuknow.co.uk/>

The Byron Report: <http://www.dcsf.gov.uk/byronreview/pdfs/Final%20Report%20Bookmarked.pdf>

The Byron Report. Children’s Summary:

<http://www.dcsf.gov.uk/byronreview/pdfs/A%20Summary%20for%20Children%20and%20Young%20People%20FINAL.pdf>

The Byron Report Executive Summary: <http://www.dcsf.gov.uk/byronreview/pdfs/Executive%20summary.pdf>

**HOME WIRELESS NETWORKS**

Wireless networks should be properly encrypted, instructions on how to do this usually come with the wireless router, failure to do so renders the account holder liable for any misuse of the internet connection associated with the unencrypted network and may allow others to see and access computers and peripheral

devices connected to it.

**LOCATION OF COMPUTER(S)**

Computers should be in a public area. It is good practice where there is a case for the computer being in a bedroom or other out of line of sight location, an agreement should be reached stating that the computer will be monitored from time to time.

**INTERNET SERVICE PROVIDER CHILD CONTROLS**

Internet or operating system child controls should be investigated and used. This may require you to set up logons at home, or separate logon accounts with your internet service provider. Most will permit a number of sub accounts. The benefits of doing so give peace of mind and will in some cases allow for usage reports to be generated. It is reasonable for users of home systems to accept that they can be monitored from time to time.

**ANTI VIRUS, SPYWARE/MALWARE**

Robust all round anti-virus/spyware/malware solutions should be in place at all times and updated frequently in line with the manufacturer’s guidance. Individuals may be liable for damage caused to other systems by malware imported from home systems.

**APPENDIX 2: E-SAFETY INCIDENT GUIDANCE/FLOW CHART**

**Where it is deemed necessary to preserve evidence of a serious breach of e-safety:**

Immediately inform the Head of School. Do not touch the computer or device in question. Any contact with the hardware may contaminate the evidence trail.

The Head of School will:

 Phone Partnership for advice (01234 798212**)** stating clearly that they have a high priority E-Safety incident and that they need to preserve an evidence trail. The Head will note the advice given to them and the name of the person they spoke to.

 If the incident involves a member of staff, they will contact their designated personnel officer for advice.

 The Head of School will inform the relevant agencies as advised by ICT or Personnel, keeping records of all conversations.

 If the event involves a child, how the Head of School responds will be dictated by the event and its origin. If the event arose in school, then contact with the parents and carers would be appropriate. However, if the event occurred within the family and has been the subject of a disclosure, referral to the LSCB is an appropriate first step.

**Where it is deemed necessary to contact external agencies**

 Keep records of who you speak to and their advice

 Follow the advice meticulously.