E-Safety Policy

September 2016

Signed by:

_____ Headteacher Date: _____

_____ Chair of governors Date: _____

Effective Practice in e-Safety

e-Safety depends on effective practice in each of the following areas:

- ◊ Education for responsible ICT use by all staff and pupils;
- ◊ A comprehensive, agreed and implemented e-Safety Policy;
- ◊ Use of a secure, filtered broadband (e.g. Broadband Sandwell);
- ◊ A school network that complies with the National Education Network standards and specifications.

The range of issues classified within e-safety is considerable, but can be categorised into three areas of risk:

Content:	being exposed to illegal, inappropriate or harmful material
Contact:	being subjected to harmful online interaction with others
Conduct:	personal online behaviour that increases the likelihood of, or causes harm

Writing and reviewing the e-Safety Policy

The e-Safety Policy is part of the School Development Plan and relates to other policies including those for ICT, bullying and for child protection:

- The school's appointed e-Safety Lead is the Headteacher.
- Our e-Safety Policy has been written by the school, building on the Sandwell e-Safety Policy. An e-safety self assessment has been completed using the 360 degree tool. The self assessment will inform agreed actions that the school will complete in order to gain the e-safety accredited mark.
- The policy has been agreed by senior management and approved by governors.
- The e-safety policy was approved by governors in: January 2017
- The next review date is (at least annually): September 2017
- Disseminated to all staff on: Available on the openhive

Teaching and Learning

Why the Internet and digital communications are 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 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.

Internet use will enhance learning:

- ◊ The school Internet access will be designed expressly for pupil use and will include 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 to research, including the skills of retrieval and evaluation.
- ◊ Pupils will be shown how to publish and present information to a wider audience.

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 the importance of cross-checking information before accepting its accuracy.
- ◊ Pupils will be taught how to report unpleasant Internet content by using the Child Exploitation and Online Protection Centre (CEOP) "Report Abuse" icon or "Hector Protector."
- ◊ Pupils will know to contact the named e-Safety lead in school if they experience any issues.

Managing Internet Access

Information system security:

- ◊ School ICT systems' security will be reviewed regularly.
- ◊ Virus protection will be updated regularly.
- ◊ Security strategies will be discussed with the Local Authority.

e-mail:

- ◊ Pupils may only use approved e-mail accounts on the school system.
- ◊ Pupils must immediately tell a teacher if they receive any form of offensive/inappropriate e-mail. The teacher must then liaise with the e-Safety Lead.
- ◊ In e-mail communication, pupils must not reveal their personal details or those of others.
- ◊ Pupils should be advised not to meet anyone first met online without specific permission or a responsible adult present.
- ◊ Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- ◊ The forwarding of chain letters is not permitted and the rationale is understood.

Published content and the school web site:

- ◊ Staff or pupil personal contact information will not generally be published.
- ◊ Only the school's office contact details should be given online.

Taking and storing images:

- ◊ Images of pupils will only be taken on school camera's
- ◊ Images need to be stored securely on devices and devices will not be removed from the school. It is important to note that images downloaded onto laptops and then subsequently deleted, although

they appear to be deleted, the file may not have been removed from the hard drive. If images of pupils need to be deleted, this needs to be referred to the ICT technician.

Publishing pupils' images and work:

- ◊ Photographs that include pupils will be selected carefully so that individual pupils cannot be identified or their image misused. (Consider using group photographs rather than full-face photos of individual children.)
- ◊ Pupils' names should not be used anywhere on the school Web site or other on-line space, particularly in association with photographs.
- ◊ Written permission from parents or carers will be obtained before photographs/digital and video images of pupils are published on the school web site.
- ◊ Work can only be published with the permission of the pupil and parents/carers.

Social networking and personal publishing:

- ◊ The school will control access to social networking sites and guidelines how to educate shareholders in their safe use are part of e-Safety policy/social networking policy.
- ◊ Where necessary, the school will closely control access to and the use of social networking sites, with consideration given as to how the pupils can be educated in their safe usage.
- ◊ Newsgroups will be blocked unless a specific use is approved.
- ◊ Pupils and staff will be advised never to give out personal details of any kind which may identify them, their friends or their location.
- ◊ Parents will be informed of their responsibilities in respect of Social Networking and the minimum age for Facebook users being 13 years old.

Managing filtering:

- ◊ The school will work with the Sandwell Local Authority and a managed filtering system (Broadband Sandwell) to ensure systems in place to protect pupils are reviewed and improved.
- ◊ If staff or pupils come across unsuitable on-line materials, the site must be reported to the e-Safety lead.
- ◊ Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Managing videoconferencing & webcam use:

- ◊ Videoconferencing should use Sandwell's broadband network to ensure quality of service and security.
- ◊ Ground rules must be established with pupils prior to videoconferencing to ensure appropriate behaviour.
- ◊ Pupils must ask permission from the supervising teacher before making or answering a videoconference call.
- ◊ Videoconferencing and webcam use will be appropriately supervised for the pupils' age.

Managing emerging technologies:

- ◊ Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before their use in school; and clear boundaries will be set.
- ◊ The senior leadership team should note that technologies such as mobile phones with wireless Internet access can bypass school filtering systems and present a new access route to undesirable material and communications.
- ◊ Staff will be issued with a school phone where contact with pupils is required or where mobile phones are used to capture photographs of pupils. Use of staff's personal mobile phones is forbidden.
- ◊ The appropriate use of VLEs/Learning Platforms will be reviewed as the technology becomes available within the school.
- ◊ The educational benefits of mobile technology need to be encouraged but not misused.

Protecting personal data:

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

Policy Decisions

Authorising Internet access:

- ◊ All staff must read and sign the Staff Code of Conduct for ICT before using any school ICT resource.
- ◊ All pupils must sign the school AUP before being granted Internet access.
- ◊ The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.
- ◊ At Key Stage 1, access to the Internet will be with adult supervision and will only access specific, approved on-line materials.
- ◊ Any person not directly employed by the school will be asked to sign a Code of Conduct before being allowed to access the internet from the school site.

Assessing risks:

- ◊ The school will take all reasonable precautions to prevent access to inappropriate 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 computer connected to the school network. Neither the school nor Sandwell Local Authority can accept liability for any material accessed or any consequences of Internet access.
- ◊ The school should audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate and effective.

Handling e-safety complaints:

- ◊ All Complaints of Internet misuse/illegal activity will be dealt with by the headteacher. All illegal activity including images will be referred immediately to the police. The Headteacher does not

need to see the evidence. **The computer/device/room should be secured. It should not be switched off, - the police should be called immediately.** Viewing material of a complaint that could potentially be illegal contaminates and possibly implicates the Headteacher in the crime. The act of opening the activity/image may change any date information stored on the computer; contaminating it.

- ◊ Complaints of a child protection nature must be dealt with in accordance with school child protection procedures. (Appendix 1 displays a flowchart of responses to an incident of concern.)
- ◊ Pupils and parents will be informed of the complaints procedure. (See schools complaints procedure.)
- ◊ Pupils and parents will be informed of consequences for pupils misusing the Internet.
- ◊ Discussions will be held with the West Midlands Police to establish procedures for handling potentially illegal issues. (West Midlands Police Non-emergencies and enquiries: Telephone: 0345 113 5000.)

Community use of the Internet:

- ◊ The school will liaise with local organisations to establish a common approach to e-safety in con junction with the e-Safety pledge.

Communications Policy

Introducing the e-Safety policy to pupils:

- ◊ e-Safety rules will be posted in all rooms where computers are used and discussed with pupils regularly.
- ◊ Pupils will be informed that network and Internet use will be monitored and appropriately followed up.
- ◊ A programme of training in e-Safety will be developed, based on the materials from the Child Exploitation and Online Protection Centre (CEOP.)
- ◊ Rewards for positive Internet use and sanctions for inappropriate Internet use both in and out of school hours are clearly stated and understood by all users.
- ◊ e-Safety training will be embedded within the ICT scheme of work or the Personal Social and Health Education (PSHE) curriculum.
- ◊ All children and young people require safe opportunities to understand the risks and benefits of the Internet and to balance these in their everyday use.

Staff and the e-Safety policy:

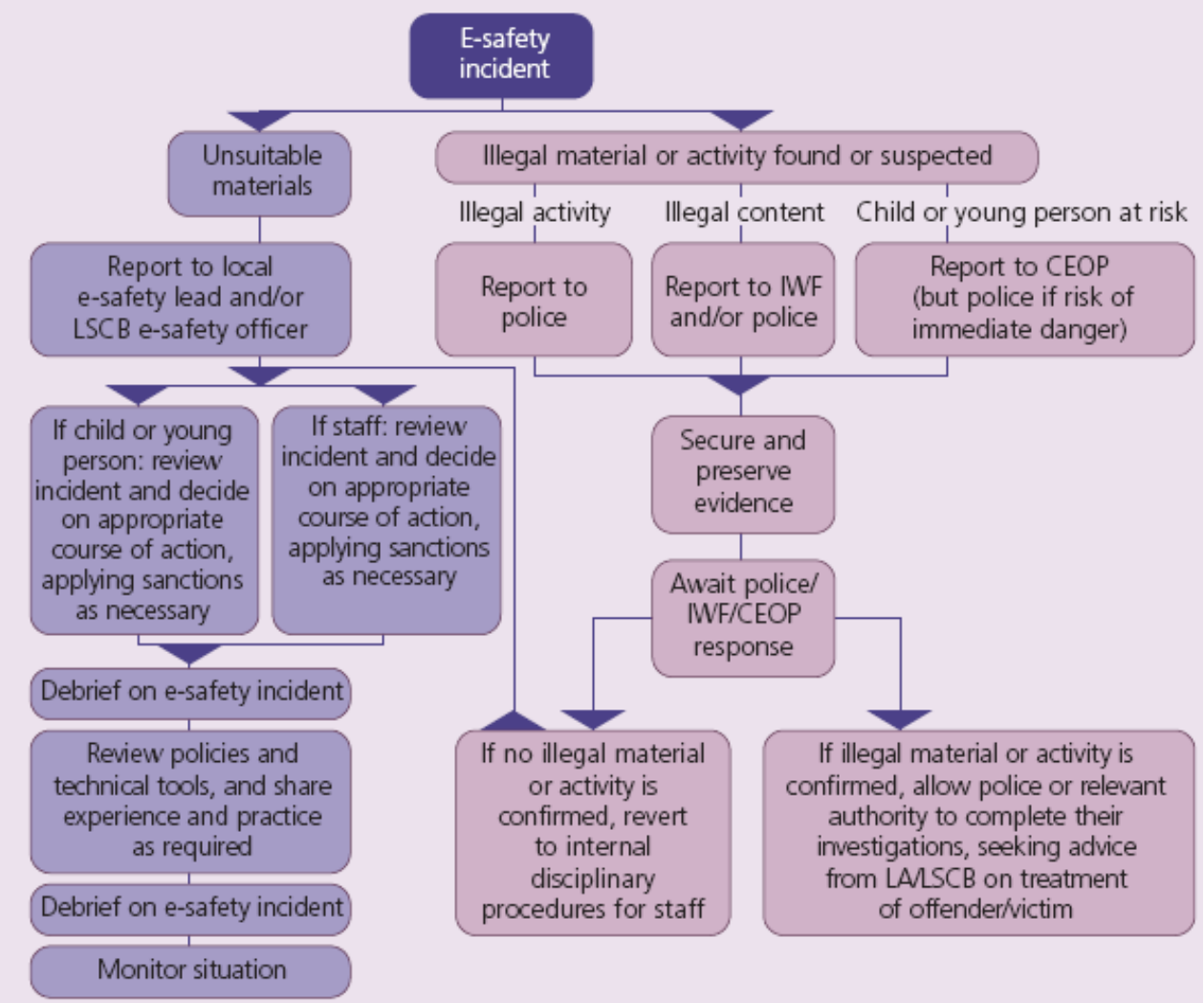
- ◊ All staff will be given the School's e-Safety policy and emphasise its importance.
- ◊ Staff must be informed that network and Internet traffic can be monitored and traced to the individual user.
- ◊ Staff that manage filtering systems or monitor ICT use will be supervised by senior management and work using the guidance and procedures for reporting issues.
- ◊ Staff will always use a child friendly, safe search engine when accessing the web with pupils e.g. "Yahoo Kids".
- ◊ Regular e-Safety training will be part of the school's Continuing Professional Development (CPD) programme.

- ◊ Buying and ordering of goods online is monitored, managed, and agreed by the Headteacher.

Enlisting parents' and carers' support:

- ◊ Parents' and carers' attention will be drawn to the school's e-Safety policy in newsletters, the school brochure and on the school's web site.
- ◊ The school will maintain a list of e-Safety resources for parents/carers.
- ◊ The school will ask all new parents to sign the parent /pupil agreement when their child is first enrolled at the school.

Appendix 1: Flowchart for responding to e-safety incidents



(Figure reproduced from Becta - *Safeguarding children online: a guide for Local Authorities and Local Safeguarding Children Boards*, page 27, appendix B)

Acceptable Use Agreement – Pupils

Child's name: _____

- I will only use ICT in school for school purposes.
- I will only use my class e-mail address or my own school e-mail address when e-mailing.
- I will only open e-mail attachments from people I know, or who my teacher has approved.
- I will not tell other people my ICT passwords.
- I will only open/delete my own files.
- I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
- I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidently find anything like this, I will tell my teacher immediately.
- I will not give out my own details such as my name, phone number or home address. I will not arrange to meet someone unless this is part of a school project approved by my teacher and a responsible adult comes with me.
- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
- I know that my use of ICT can be checked and that my parent/carer will be contacted if a member of school staff is concerned about my eSafety.

Signed: _____ Date: _____

Burnt Tree Primary School
Hill Rd, Tividale, Oldbury, B69 2LN
Tel 0121 557 2967 Fax 0121 522 4980

Head Teacher Mrs. J. Evans

Dear Parent/Carer

ICT including the internet, e-mail and mobile technologies etc has become an important part of learning in our school. We expect all children to be safe and responsible when using any ICT.

Please read and discuss the attached eSafety rules with your child and return the attached rules signed by your child and the slip at the bottom of this letter. The school's e-safety policy can be found on the school's website or a copy can be obtained from the school office.

Parents are reminded of their responsibility in respect of Social Networking and that that the minimum age for facebook users is 13 years old.

Thank you for your continued support.

Yours sincerely

Mrs J Evans
Headteacher

I/We have discussed the attached eSafety with my/our child.

_____ (child's name) agrees to follow the eSafety rules and to support the safe use of ICT at Burnt Tree Primary School.

Parent/Carer Signature: _____

Date: _____

Appendix 4

Staff, Governor and Visitor Code of Conduct for ICT

To ensure that members of staff, governors and visitors are fully aware of their professional responsibilities when using information systems and when communicating with pupils, they are asked to sign this code of conduct. The school's e-safety policy should be read for further information and clarification.

I appreciate that ICT includes a wide range of systems, including mobile phones, PDAs, digital cameras, email, social networking and that ICT use may also include personal ICT devices when used for school business.

I understand that school information systems may not be used for private purposes without specific permission from the Head Teacher and that it may be a criminal offence to use a school ICT system for a purpose not permitted by its owner. The maximum punishment for breaking this law is a £5000 fine or several years' imprisonment.

I understand that my use of school information systems, Internet and email may be monitored and recorded to ensure policy compliance.

I will respect system security and I will not disclose any password or security information to anyone other than an authorised system manager.

I will not install any software or hardware without permission.

I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.

I will ensure that personal data is stored securely and is used appropriately, whether in school, taken off the school premises or accessed remotely.

Images of pupils and/or staff will only be taken, stored and used for professional purposes in line with the school policy and with written consent of the parent/carer or staff member. Images will not be distributed outside the school network without the permission of the parent/carer or staff member and the Headteacher.

I will respect copyright and intellectual property rights.

I will report any incidents of concern regarding children's safety to the e-Safety Coordinator, the Designated Child Protection officer / Head Teacher.

I will ensure that electronic communications with pupils including email, IM and social networking are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.

I will promote e-safety with students in my care and will help them to develop a responsible attitude to system use, communications and publishing.

I will not give out my own personal, such as mobile phone number and personal e-mail address to pupils.

The school may exercise its right to monitor the use of the school's information systems and Internet access, to intercept e-mail and to delete inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

I have read, understood and accept this Code of Conduct for ICT.

Signed: ..... Date: .....

Full Name: ..... (Printed)

Job Title/Role: .....

Appendix 5: Useful resources for teachers

BBC Stay Safe
www.bbc.co.uk/cbbc/help/safesurfing

Chat Danger
www.chatdanger.com

Child Exploitation and Online Protection Centre
www.ceop.gov.uk

Childnet
www.childnet-int.org

Cyber Café
http://thinkuknow.co.uk/8_10/cybercafe/cafe/base.aspx

Digizen
www.digizen.org

Kent e-Safety Policy and Guidance, Posters etc
www.clusterweb.org.uk/kcn/e-safety_home.cfm

Kidsmart
www.kidsmart.org.uk

Safer Children in the Digital World
www.dfes.gov.uk/byronreview

Solihull e-Safety Policy
http://www.solihull.gov.uk/Attachments/e-safetycurriculum.pdf

Think U Know
www.thinkuknow.co.uk

Appendix 6: Useful resources for parents

Care for the family
www.careforthefamily.org.uk/pdf/supportnet/InternetSafety.pdf

Childnet International "Know It All" CD
http://publications.teachernet.gov.uk

Family Online Safe Institute
www.fosi.org

Internet Watch Foundation
www.iwf.org.uk

Kent leaflet for parents: Children, ICT & e-Safety
www.kented.org.uk/ngfl/ict/safety.htm

Parents Centre
www.parentscentre.gov.uk

Internet Safety Zone
www.internetsafetyzone.com