Devonshire Academies E-safety Policy

October 2017

Based on Sandwell Local Authority E-safety Policy Guidance

Aims of the Policy

- *To protect the school ICT systems/equipment and users from misuse*
- *To ensure that pupils and staff are responsible users and stay safe whilst using ICT equipment in school*

Teaching and Learning

The Internet is an essential resource 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 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 how to use the Internet safely and appropriately.
- ➢ 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 what to do if they experience any issues whilst online.

Writing and reviewing the e-Safety Policy

This e-Safety Policy is part of the School Development Plan. It has been written by the school based on the Sandwell e-Safety Policy guidelines, agreed by senior management and approved by governors.

- The e-Safety Policy was revised by: Elise Waldron/Sharon Gibson
- It was approved by the Governors on: ____________________
- The next review date is (at least annually): October 2018
- Disseminated to all staff on November 2017

Managing Internet Access

Information system security:

- School ICT systems' security will be reviewed regularly.
- Virus protection will be updated regularly.

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.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- The school should consider how e-mail from pupils to external bodies is presented and controlled (e.g. cc messages to "*esafety@school.com")*
- The forwarding of chain letters is not permitted

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.
- The content will be checked and monitored regularly to ensure that it is accurate and appropriate.

Publishing pupils' images and work:

- Written permission from parents or carers will be obtained before photographs/digital and video images of pupils are published on the school web site.
- Photographs that include pupils will be selected carefully
- Work can only be published with the permission of the pupil and parents/carers.
- Pupil image file names will not refer to the pupil by name.

Social networking and personal publishing:

- The school will control access to social networking sites
- Pupils and parents will be strongly advised of the age restrictions and that the use of social network spaces outside school brings a range of dangers to all pupils.
- Pupils and staff will be advised never to give out personal details of any kind which may identify them, their friends or their location.

Managing filtering:

- The school will work with 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 Coordinator.
- 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 (including making or answering a 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.
- The educational benefits of mobile technology need to be encouraged but not misused.
- When mobile technology is used in the classroom, clear ground rules must be established for appropriate use.
- Use of staff's personal mobile phones to take photos of children is forbidden.
- Pupils will be given a username and password to access RM Unify (VLE), which is managed by staff.

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:

- Staff will be required to read sign the **Staff ICT and Internet Usage Policy** annually.

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.

Handling e-safety complaints:

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the headteacher.
- 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 consequences for pupils misusing the Internet.

Community use of the Internet:

- The school will liaise with local organisations, such as the Police (Community Police Officers) to establish a common approach to e-safety in conjunction with the e-Safety pledge.

Communications Policy

Introducing the e-Safety policy to pupils:

- e-Safety rules will be displayed in the ICT suite and discussed with pupils regularly.
- Pupils will be informed that network and Internet use will be monitored and sanctions given for inappropriate use.
- E-Safety in school will be developed based on the materials from the Child Exploitation and Online Protection Centre (CEOP.)
- e-Safety training will be embedded within the 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 access to 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 will try to 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.

Enlisting parents' and carers' support:

- Parents' and carers' attention will be drawn to the school's e-Safety policy in newsletters and on the school's web site.
- The school will maintain a list of e-Safety resources for parents/carers.
- e-Safety support, guidance, advice and/or workshops will be offered to parents/carers.

** ** **

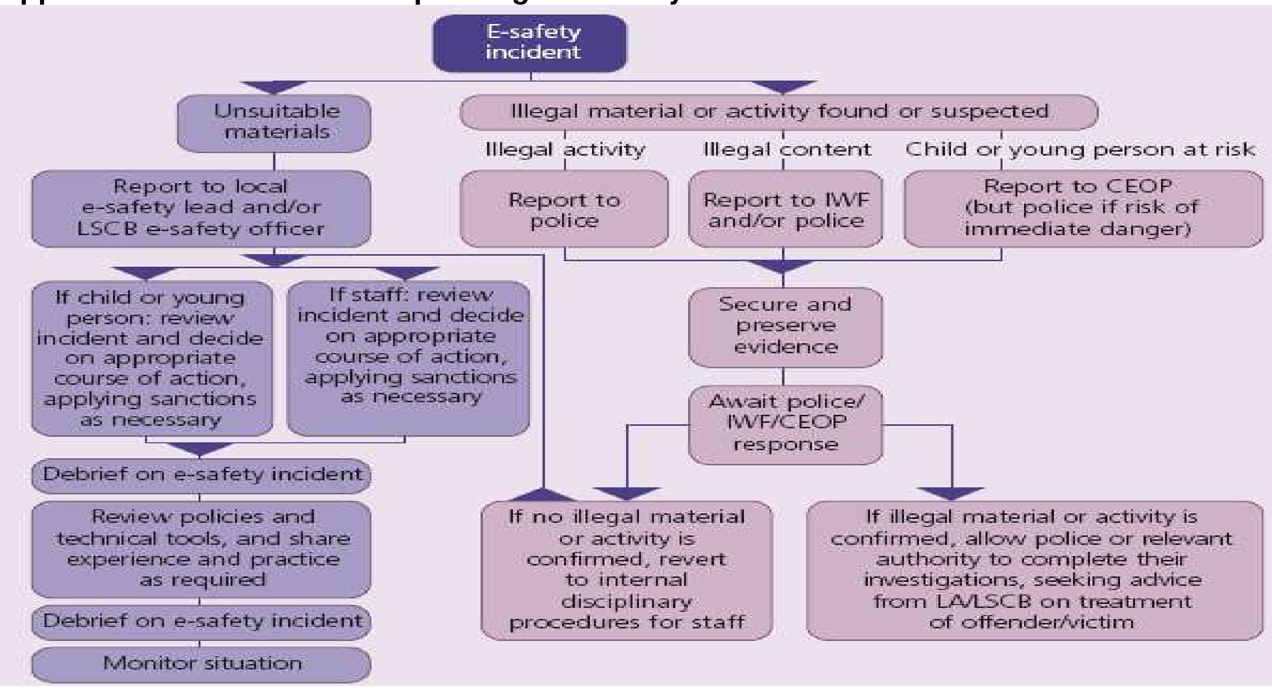
Disclaimer

The school will take all reasonable precautions to ensure that users access appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. The school cannot accept liability for the material accessed, or any consequences resulting from Internet use.

E-Safety Audit

Has the school an e-Safety Policy in conjunction with Sandwell Local Authority?		Y
The school e-safety policy was agreed:		
The policy is available for staff on Community Chest and in the staffroom		
The policy is available for parents/carers:	http://www.devonshireinfantacademy.org/	
The responsible member of the Senior Leadership Team is:	Sharron Philpot/Sharon Gibson	
The responsible member of the Governing Body is:	Gurinder Josan	
The Designated Child Protection Coordinator is:	Sharron Philpot/Sharon Gibson	
The e-Safety lead in school is:	Sharron Philpot	
Has e-safety training been provided for pupils? Embedded in curriculum		Y
Has e-safety training been provided for staff? February 2015 and reminders Oct 2016 – E-safety resources		Y
Is there a clear procedure for a response to an incident of concern?		Y
Have e-safety materials been obtained from recommended providers?		Y
Do all staff sign a Code of Conduct for ICT on appointment?		Y
Are all pupils aware of the School's e-Safety rules?		Y
Are e-Safety rules displayed in all rooms where computers are used and expressed in a form that is accessible to all pupils?		Y
Are staff, pupils, parents/carers and visitors aware that network and Internet use is closely monitored and individual usage can be traced?		Y
Has an ICT security audit been initiated by the Senior Leadership Team, possibly using external expertise? Labels/extra alarms		Y
Is personal data collected, stored and used according to the principles of the Data Protection Act?		Y
Is Internet access provided by an approved educational Internet service provider which complies with DfE requirements (e.g. Broadband Sandwell)?		Y
Has the school-level filtering been designed to reflect educational objectives and approved by the Senior Leadership Team?		Y
Is anti-virus up-to-date, and installed on all devices? New Anti-virus purchased for 3 years – review May 2017		Y
Are all shareholders aware of the CEOP Report Abuse button?		Y

Appendix 1: Flowchart for responding to e-safety incidents


E-safety incident
Unsuitable materials
Illegal material or activity found or suspected
Illegal activity
Illegal content
Child or young person at risk
Report to local e-safety lead and/or LSCB e-safety officer
Report to police
Report to IWF and/or police
Report to CEOP (but police if risk of immediate danger)
If child or young person: review incident and decide on appropriate course of action, applying sanctions as necessary
If staff: review incident and decide on appropriate course of action, applying sanctions as necessary
Secure and preserve evidence
Await police/ IWF/CEOP response
Debrief on e-safety incident
Review policies and technical tools, and share experience and practice as required
Debrief on e-safety incident
Monitor situation
If no illegal material or activity is confirmed, revert to internal disciplinary procedures for staff
If illegal material or activity is confirmed, allow police or relevant authority to complete their investigations, seeking advice from LA/LSCB on treatment of offender/victim

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

Appendix 2: 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

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