Lightwoods School

Policy Library

TITLE:

Lightwoods e-Safety Policy

L031

Table of Contents

1. Introduction

As the use of online services and resources grows, so has awareness of the risks and potential dangers which arise from the use of communications technology and the internet. Those risks are not confined to the use of computers; they may also arise through the use of other devices such as games consoles and mobile phones.

Our E-safety and ICT Acceptable Use Policy (AUP) has been written in line with LA and government guidance and is agreed by the Governing body and the Senior Management Team. It will be reviewed annually.

Use of the school's ICT equipment by any members of the school community must be in accordance with this policy. Any use which infringes this policy will be treated very seriously by the School Governing Body.

2. 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. TrustNet)
- A school network that complies with the National Education Network standards and specifications.

3. 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 e-safety lead and DSL roles overlap.
  It is not a technical role.
- Our e-Safety Policy has been written by the school, building on the Sandwell e-Safety Policy. It has been agreed by senior management and approved by governors.
- The school's e-safety lead is Mr. Nigel Roberts

E-Safety Audit

Has the school an e-Safety Policy in conjunction with Sandwell Local Authority?	**Y / N**
Date of latest update (at least annual): Autumn 2019	
The school e-safety policy was agreed on:	
The policy is available for staff at:	
The policy is available for parents/carers at:	
The responsible member of the Senior Leadership Team is: Nigel Roberts/Jenny Wright	
The responsible member of the Governing Body is:	
The Designated Child Protection Coordinator is: Nigel Roberts	
The e-Safety lead in school is: Nigel Roberts	
Has e-safety training been provided for pupils?	**Y / N**
Has e-safety training been provided for staff?	**Y / N**
Is there a clear procedure for a response to an incident of concern?	**Y / N**
Have e-safety materials been obtained from recommended providers?	**Y / N**
Do all staff sign a Code of Conduct for ICT on appointment?	**Y / N**
Are all pupils aware of the School's e-Safety rules and acceptable use policy?	**Y / N**
Are e-Safety rules displayed in all rooms where computers are used and expressed in a form that is accessible to all pupils?	**Y / N**
Do parents/carers sign and return an agreement that their child will comply with the School e-Safety rules and acceptable use policy?	**Y / N**
Are staff, pupils, parents/carers and visitors aware that network and Internet use is closely monitored and individual usage can be traced?	**Y / N**
Has an ICT security audit been initiated by the Senior Leadership Team, possibly using external expertise?	**Y / N**
Is personal data collected, stored and used according to the principles of the Data Protection Act?	**Y / N**
Is Internet access provided by an approved educational Internet service provider which complies with Department for Children, Schools and Families (DCSF) requirements (e.g. Broadband Sandwell)?	**Y / N**
Has the school-level filtering been designed to reflect educational objectives and approved by the Senior Leadership Team?	**Y / N**
Is anti-virus up-to-date, and installed on all devices?	**Y / N**
Are all shareholders aware of the CEOP Report Abuse button?	**Y / N**

4. The Importance of Internet use in Education

The purpose of Internet use in school is to raise educational standards, to promote student achievement, to support the professional work of staff and to enhance the school's management information and business administration systems.

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 and know the immediate procedures including alerting supervising staff and turning off the monitor etc.

5. Managing Internet Access

Information system security**:**

- School ICT systems' security will be reviewed regularly.
- Virus protection will be kept up to date.
- 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 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 and the rationale is understood.

Published content and the school website:

Staff or pupil personal contact information will not generally be published.
Only the school's office contact details should be given online.
The Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

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.
- Ideally pupils would only ever use moderated social networking sites.
- Pupils and parents will be strongly advised that the use of social network spaces outside school brings a range of dangers to all pupils.
- Pupils will be advised to use nicknames and avatars when using social networking sites.
-

Managing filtering:

- The school will work with the Sandwell Local Authority and a managed filtering system via TrustNet 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 TrustNet to ensure quality of service and security.
- Ground rules must be established with pupils prior to videoconferencing to ensure appropriate behaviour.
- Pupils wont video conference
- 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.
- When mobile technology is used in the classroom, clear ground rules must be established for it's appropriate use.
- Mobile phones will not be used during lessons or formal school time (with the exception of educational use and agreed with the teacher/school).
- The sending of abusive or inappropriate text messages or files by Bluetooth or any other means is forbidden.
- The use by pupils of cameras in mobile phones will be kept under review.
- Games machines including the Sony PlayStation, Microsoft Xbox and others have Internet access which may not include filtering. Care is required in any use in school or other officially sanctioned location.
- 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.

6. Photographic and Video Images

There are many occasions on which it is a good thing to make use of photographs and video images that include children. This is perfectly proper and to be encouraged. However, our school will do all it can to ensure that images are used properly, and that, as in all matters, risks are minimised, and our children kept safe and secure, whether at school or elsewhere. The aim of this policy is to establish the right balance between the proper use of technology and the safety of our children at all times.
Under the terms of the Data Protection Act 1998, all photographs and video images of children and staff alike are classified as personal data. This means that no image can be used for display or for school publicity etc., unless consent is given by or on behalf of the individual concerned.

Parental permission

- All parents and carers will be asked to sign a consent form allowing their child to be photographed or videoed while taking part in school activities, and for the image to be used within the school. This form will be given to the parents or guardians of all children joining the school in each successive year. This 'rolling' consent will allow the school to take pictures of pupils engaged in educational activities such as sports events, drama productions, field trips, etc., and to use these pictures internally. Where parents or carers do not give their consent, then the children concerned will not have pictures taken of them.
- All pictures taken will be appropriate, and will show children properly clothed for the activity they are engaged in. The school will do all it can to ensure that due sensitivity is shown in the choice and composition of these images.

School performances

- We will allow video and photographic recordings of all school performances, as long as the parents or guardians of the children involved have given their consent.
- The school will observe the way in which video recordings are made, and photographs taken, during performances, and will withdraw the right of anyone to bring a camera of any sort if they are felt to be making inappropriate images. For example, photography is forbidden in changing rooms or backstage during school productions. Those making recordings or taking pictures will be reminded on their use for personal record.

The Internet

- Only appropriate images will be used on the school Internet site, and children will not be identified by their name or address on the school website.
- Images of children will only be used on external platforms where consent is given to that individual

Mobile phones

- With the exception of Y6 pupils who walk to or from school unaccompanied, we do not allow children to bring mobile phones into school. Adults may bring mobile phones, but must not use them to take pictures of children.

Use of digital cameras

- There are many ways in which the use of digital images is valuable for children's learning. For example, they may be used in art work or geography or science fieldwork and for evidence of pupil learning.
- Images will be made only as appropriate for school-related activities.
- Children will be taught how to take pictures, but we will discourage them from taking pictures of each other, other than for specific projects. They will be supervised by an adult when they have access to a digital camera.
- All images will be stored safely as a record of school activity on password protected machines.

Publishing Pupil Images and Media publications

Sometimes, local or national media visit the school to follow up a news story.
This is often to do with a notable achievement by a child or a group of children from the school. For example, the netball team may have won a regional competition, or the school may have raised money for a charity whose representative wants to receive the donation in person. In this situation, where children's images might be made public, the school will only allow pupils with parental permission for external use of photographs to be photographed and will inform the parents of the publication. Newspapers normally ask for the names of the children to go alongside the photographs; if parents or carers do not wish this to happen, then the school will not allow the individual to be photographed or filmed by the media concerned.

- 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 a school Website 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.
- Pupil image file names will not refer to the pupil by name.
- Parents should be clearly informed of the school policy on image taking and publishing, both on school and independent electronic software repositories.

7. 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.
- Parents and carers will be asked to sign and return a consent form. If forms not returned, Parent/Carer interviews to be arranged.
- Any person not directly employed by the school will be asked to sign a Staff Code of Conduct before being allowed to access the internet from the school site.
- A sample Staff Code of Conduct is available on Sandwell's e-Safety Website.

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:

- 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 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: Tel: 0345 113 5000

Community use of the Internet:

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

8. Communications

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:

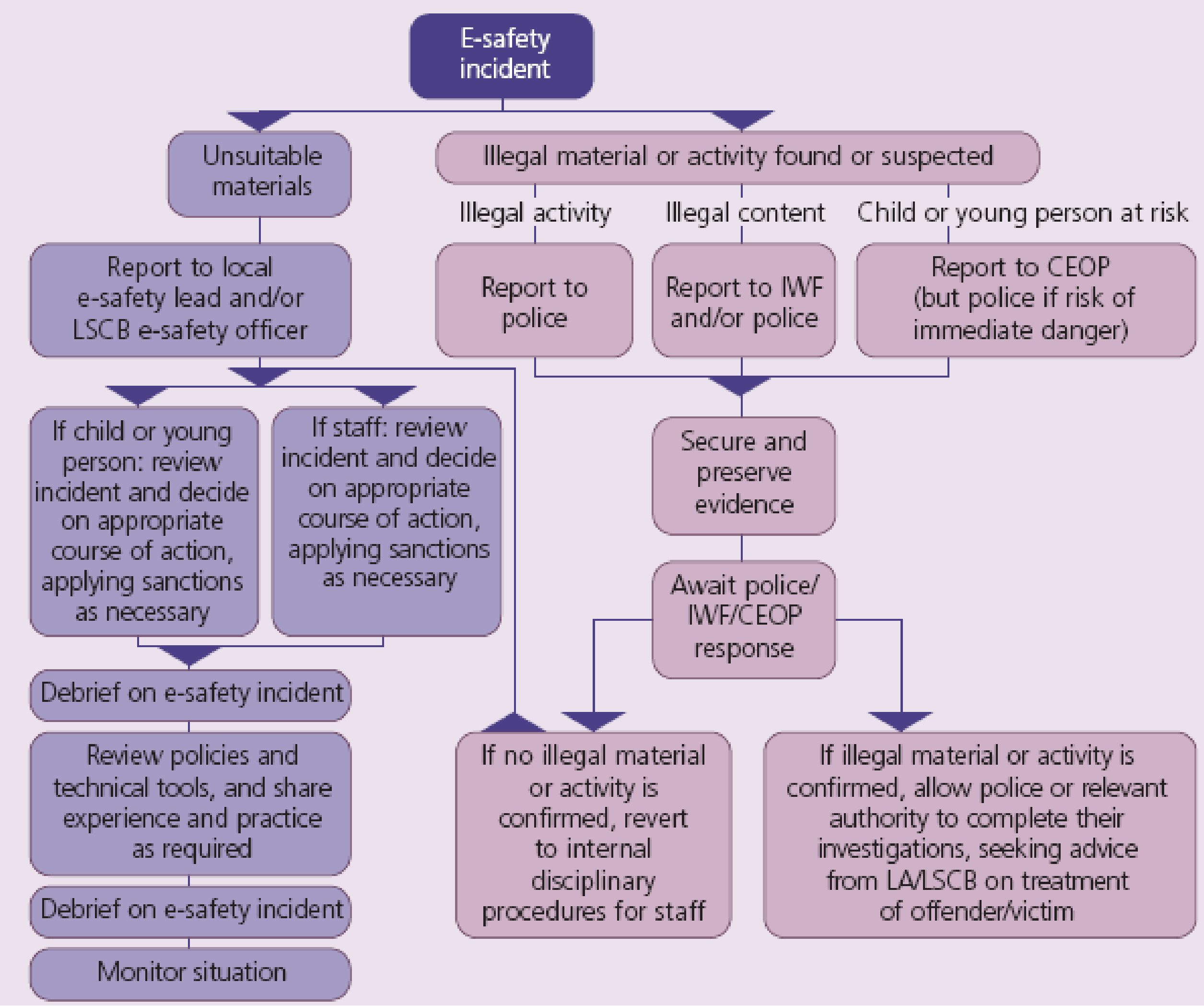
- Parents' and carers' attention will be drawn to the school's e-Safety policy in newsletters, the school brochure and on the school's web site.
- The school will maintain a list of e-Safety resources for parents/carers.
- The school will ask all new parents to sign the parent /pupil agreement when they register their child with the school.
- e-Safety support, guidance, advice and/or workshops will be offered to parents/carers with an e-Safety support contact available on the school's website.

Monitoring

This policy will be monitored by the governing body and revised as appropriate, and not less than two years from the date of its adoption.

- Any incidents of concern relating to this policy will be referred to the Chair of Governors by the headteacher.

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

Appendix 3: 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

TrustNet
http://www.igfl.net/downloads/online-safety/LGFL-OS-Appropriate-Filtering-for-education-settings-provider-Response-June-2016.pdf