Leighswood School

E-Safety Policy

Completed By:	**B Barley**
Date Completed:	**Autumn 2015**
Agreed by Staff:	**Spring 2016**
Agreed by Governors:	**Spring 2016**
To be reviewed:	**Autumn 2018**

LEIGHSWOOD SCHOOL

E-SAFETY POLICY

Rationale

E-safety encompasses Internet technologies and electronic communications such as mobile phones as well as collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

The internet is an essential element in 21st century life for education, business and social interaction. It allows for educational establishments to link together, share resources and work on educational projects to generate cohesion where best practice will help our school to improve. Internet use is a part of the statuary curriculum and a necessary tool for staff.

New technology, new risks

New technology may expose any user to risk.

- **content:** being exposed to illegal, inappropriate or harmful material (pornography, violence, racist language, scams)
- **contact:** being subjected to harmful online interaction with other users (cyberbullying, identity theft, grooming)
- **conduct:** personal online behaviour that increases the likelihood of, or causes, harm to self or others (disclosure of personal information, damaging digital footprint, breaches of copyright law or plagiarism, poor well-being due to over-use)

Purpose

The school will maintain a policy that ensures that full use of the Internet is made to support children's learning while minimising accidental or deliberate misuse. This will include provision of guidelines for staff and appointing an e-safety co-ordinator. The policy relates to other policies including the Anti-Bullying policy, Child Protection Policy and Photographic Policy.

Working together to be e-safe

E-safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and pupils
- Sound implementation of e-safety policy
- Safe and secure broadband provided by LA ICT including effective management of Netsweeper filtering
- Parents understanding the benefits and risks of technology and maintaining e-safety practices out of school

Teaching and Learning

A filtered Internet service is designed expressly for pupil use and will be used at all times to reduce the possibility of accessing unsuitable materials. All students have internet access via a filtered proxy server. This filters out inappropriate content as well as chatrooms, YouTube, social networking sites and forums where free comments can be posted.

Pupils' access to the Internet and electronic mail will be supervised by a responsible adult at all times. 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 in research, including the skills of knowledge location, retrieval and evaluation.

The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.

Pupils should be taught to be critically aware of the materials they read and encouraged to validate information before accepting its accuracy.

Raising awareness of e-safety

Whole school awareness will be raised during Safer Internet Day (February) when children and adults will sign or renew an age-appropriate AUP policy. E-safety tips will be shared and revisited regularly (See appendix C). E-safety will also be taught and revisited regularly through skills based ICT lessons and during other lessons where use of technology plays a part. Circle time will provide an open forum for discussing e-safety issues children may face.

E-safety rules are posted in all rooms where there is computer access and referred to regularly.

Reporting mechanisms

The school ICT systems security will be reviewed regularly in line with Walsall Children's Services requirements. If staff or pupils discover unsuitable material it must be reported to the named e-safety coordinator.

What will happen at Leighswood if staff or pupils are exposed to unsuitable material online?

- E-safety coordinator informed and incident recorded.
- LA ICT contacted, website blocked if url known.
- Support offered to pupil/staff member and parents informed as appropriate.

Pupils may only use approved e-mail accounts on the school system and must not reveal any personal details about themselves or others. Email sent to external organisations should be written carefully and authorised before sending.

Virus protection will be updated regularly in line with Walsall Children's Services requirements.

Internet Misuse

Any deliberate misuse of communication technology or Internet services will be treated as a serious breach of school rules.

What will happen at Leighswood if communication technology or Internet services are deliberately misused?

- Dealt with by a senior member of staff and appropriate sanctions imposed.
- A record will be kept on Sims
- Parents will be informed

Everyone will be made aware that Internet traffic can be monitored and traced to the individual user.

Staff or pupil personal contact information will not generally be published. The contact details given online are postbox@leighswood.walsall.sch.uk

Photographs that include pupils will be selected carefully so that individual pupils cannot be identified or their image misused. If a photograph is used then naming the pupil will be avoided wherever possible. Policy for the use of photographs should be adhered to.

Work can only be published with permission of the pupil.

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

Sharing our e-safety policy with parents and the wider community

The school's e-safety policy should be made known to the parents and displayed via the school website. Links to useful websites will accompany this policy (see appendix D). School will take their role in educating parents about e-safety seriously by providing information and awareness sessions.

Acceptable Use Policies

Age appropriate Acceptable Use Statements for all users must be adhered to (See appendix B).

Any person not directly employed by the school will be asked to read and sign the Acceptable Use Statement before being allowed access to the internet from the school site.

Minimised risk

The school will take all reasonable precautions to ensure that users access only appropriate 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 school computer. Neither the school nor LA ICT can accept liability for the material accessed, or any consequences of Internet access.

In the event of any parent expressing concern over pupil access to the Internet or electronic mail, then a letter of explanation should be offered. (See appendix A)

APPENDIX A

Dear Parent,

Access to the Internet in School

The school provides access to a range of information sources, including the Internet. The Internet enables pupils to explore thousands of sources of information and to exchange messages with other Internet users across the world. The aim of this is to further educational goals and objectives and enhance personalised learning opportunities. We believe that the Internet can make a significant contribution to your child's education.

However, the Internet can also provide access to less desirable information, therefore we:

- supervise pupils' access to the Internet and electronic mail services;
- treat any deliberate misuse of the Internet or electronic mail services as a serious breach of school rules and report it to parents;
- use an Internet Service Provider which filters out sources of undesirable materials as soon as they are reported so they can no longer be accessed.

We believe that these measures let pupils gain the benefits of using the Internet for educational purposes while minimising the risk of them accessing inappropriate materials.

During school, teachers will guide pupils toward appropriate materials. Outside of school, families bear the same responsibility for such guidance as they exercise with information sources such as television, telephones, films, radio and other potentially offensive material.

Yours sincerely,

APPENDIX B

AUP Guidance notes for learners in KS1

I want to feel safe all the time.

I agree that at school and at home I will:

- always keep my passwords a secret
- only open pages which my teacher or parent/carer has said are OK
- only chat with people I know in real life
- tell my teacher or my parent/carer if anything makes me feel scared or uncomfortable
- make sure all messages I send are polite
- show my teacher or my parent/carer if I get a nasty message
- not reply to any nasty message or anything which makes me feel uncomfortable
- not give my mobile phone number to anyone who is not a friend in real life
- only email people I know or if my teacher or parent/carer agrees
- talk to my teacher or parent/carer before using anything on the internet
- not tell people about myself online (I will not tell them my name, anything about my home and family and pets)
- never agree to meet a stranger
- only install apps when a grown up agrees

Anything I do on the computer may be seen by someone else

I know about the CEOP report button and know when to use it

Signed Date

AUP Guidance notes for learners in
KS2

When I am using the computer or other technologies,
I want to feel safe all the time.

I agree that at school and at home I will:

- always keep my passwords a secret
- only visit sites which are appropriate to my work at the time
- make sure all messages I send are respectful
- show a responsible adult if I get a nasty message or get sent anything that makes me feel uncomfortable
- not reply to any nasty message or anything which makes me feel uncomfortable
- only give my mobile phone number to friends I know in real life
- not use my mobile device in school or in the school grounds
- only use email which has been approved by school
- only email people I know or those approved by a responsible adult
- only use my school email when I am in school, and no other account
- discuss and agree my use of a social networking site with a responsible adult before joining
- always keep my personal details private. (My name, family information, journey to school, my pets and hobbies are all examples of personal details)
- always check with a responsible adult and my parents/carers before I show photographs of myself or others
- only create and share content that is legal
- never meet an online friend
- never install an app without adult permission

I know that once I post a message or an item on the internet then it is completely out of my control and I am responsible for the message.

I know that anything I write or say on any website that I visit may be being viewed by a responsible adult and monitored.

I am aware of the CEOP report button and know when to use it

Signed Date

AUP Guidance notes for adults working with young people

The policy aims to ensure that any communications technology is used without creating unnecessary risk to users while supporting learning.

I agree that I will:

- only use, move and share personal data securely
- respect the school network security by logging off when I am away from my computer
- educate pupils in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation
- educate pupils in the recognition of bias, unreliability and validity of sources
- actively educate learners to respect copyright law and intellectual property rights of others
- only use approved e-mail accounts
- only use pupil images or work that will not enable individual pupils to be identified
- only give permission to pupils to communicate on line with trusted users
- use the ICT facilities sensibly, professionally, lawfully, consistent with my duties and with respect for pupils and colleagues
- not share or use my personal (home) accounts/data (e.g. Facebook, email, ebay etc.) with pupils
- only use pupil images when approved by parents and in a way that will not enable individual pupils to be identified on a public facing site.
- set strong passwords – a strong password is one which uses a combination of letters, numbers and other permitted signs
- report unsuitable content or activities to the e-safety coordinator
- ensure that videoconferencing is supervised appropriately for the learner's age
- pass on any examples of Internet misuse to a senior member of staff
- post and promote any supplied e-safety guidance appropriately

I agree that I will not:

- visit Internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:
  - pornography (including child pornography)
  - promoting discrimination of any kind
  - promoting racial or religious hatred
  - promoting illegal acts
  - breaching any Local Authority/School policies, e.g. gambling
  - doing anything which exposes children to danger
  - any other information which may be offensive to colleagues
- forwarding chain letters
- breaching copyright law
- using personal digital recordings equipment including cameras or other devices for talking/transferring images of pupils or staff without permission.
- Storing images or other files off site without permission from the Headteacher.

I will ensure that any private social networking sites, blogs, etc that I create or actively contribute to, do not compromise my professional role.

I understand that data protection policy requires me to keep any information I see regarding staff or pupils which is held within the school's management information system private, secure and confidential. The only exception is when there is a safeguarding issue; I am required by law to disclose such information to an appropriate authority.

I accept that my use of the school and Local Authority ICT facilities may be monitored and the outcomes of the monitoring may be used.

Signed: Date:

AUP Guidance notes for schools and governors

The policy aims to ensure that any communication technology (including computers, tablets and mobile phones etc.) is used to support learning without creating unnecessary risk to users.

The governors will ensure that:

learners are encouraged to enjoy the safe use of digital technology to enrich their learning;

learners are made aware of risks and processes for safe digital use;

all adults and learners have received the appropriate acceptable use policies and any required training;

the school has appointed an e-safety coordinator and a named governor takes responsibility for e-safety;

an e-safety policy has been written by the school, building on the LSCB e-safety policy and BECTA guidance;

the e-safety policy and its implementation will be reviewed regularly;

the school internet access is designed for educational use and will include appropriate filtering and monitoring;

copyright law is not breached;

learners are taught to evaluate digital materials appropriately;

parents are aware of the acceptable use policy;

parents will be informed that all technology usage may be subject to monitoring, including URLs and text;

the school will take all reasonable precautions to ensure that users access only appropriate material;

the school will audit use of technology (using the 360 degrees Self-Review Framework) to establish if the e-safety policy is adequate and appropriately implemented;

methods to identify, assess and minimise risks will be reviewed annually;

complaints of internet misuse will be dealt with by a senior member of staff.

APPENDIX C

Top Ten E-Safety Tips for discussion

- Always think of your personal safety first when using ICT or your mobile phone. Remember it is easy for anyone to lie about who they are online, so you can never really be sure about who you are talking to.
- Do not give out any personal information about yourself online to people you do not know. This includes your full name, address, street name, postcode, or school name. Only ever give out your location as Walsall.
- Never give your contact number to anyone who you don't know.
- It's a good idea to use a nickname rather than your real name.
- Don't meet people that you have only spoken to online. If you do decide to meet up with anyone in real life then make sure you take a trusted adult with you and meet in a public place at a busy time.
- Never give out pictures online or over a mobile unless you know the person in real life. It is easy for people to take your pictures and alter them, send them on, or even pretend to be you with them.
- Always use private settings whenever you are setting up a social networking page or an Instant Messenger (IM) account. This is so people who you don't want to see your profile can't
- Anything you post or upload to the internet is there forever so be very careful what you put online.
- Never go onto webcam with people you don't know in real life. Webcam images can be recorded and copied and also shared with other people.
- If you receive any messages or pictures that worry or upset you talk to an adult you trust. You may also report it online, via the thinkuknow website http://www.thinkuknow.co.uk.

Appendix D

Further e-safety information and guidance

Think U Know website (report abuse)
http://www.thinkuknow.co.uk/

Child Exploitation & Online Protection Centre
http://www.ceop.gov.uk/

Information for children
http://www.kidsmart.org.uk/
http://www.bbc.co.uk/cbbc/topics/stay-safe

Further information for Young people, parents and teachers
http://www.saferinternet.org.uk/

Safety tips for parents
http://www.bbc.co.uk/cbeebies/grownups/article/internet-use-and-safety/
http://www.bbc.co.uk/webwise/0/