Longwill
a primary school for Deaf children

LONGWILL SCHOOL FOR DEAF CHILDREN

E-SAFETY POLICY

January 2022

Rationale

Birmingham LA and Longwill School believes in the educational benefits of curriculum internet use. The school recognises that there are risks and dangers associated with inappropriate use and so plans accordingly to ensure appropriate, effective and safe pupil use.

Our E-Safety Policy covers the safe use of Internet and electronic communications technologies such as Microsoft Teams, mobile phones, iPads and mobile learning devices, emerging technologies and wireless connectivity. The policy highlights the need to educate children and young people about the benefits and risks of using new technologies both in and away from school. It will also provide safeguards and rules to guide all users whether staff or student in their online experiences.

E-safety is viewed as part of our wider safeguarding and child protection policies and our commitment to protecting rights of children as a Unicef Rights Respecting school; and not simply a matter limited to Computing.

Article 17
You have the right to get information that is important to your well-being, from radio, newspaper, books, computers and other sources.

Core Principles of Internet Safety

The Internet has become an everyday part of most people's lives and its effective use is an essential life-skill. Unmediated internet access brings with it the possibility of placing pupils in embarrassing, inappropriate and even dangerous situations. Therefore, we need a policy to help to ensure responsible use and the safety of pupils. This E-Safety Policy is built on the following five core principles:

- **Guided Educational Use**

  Significant educational benefits should result from curriculum internet use including access to information from around the world and the abilities to communicate widely and to publish easily. Curriculum internet use should be planned, task-orientated and educational within a regulated and managed environment. Directed and successful internet use will also reduce the opportunities for activities of dubious worth.

- **Risk Assessment**

  21st century life presents dangers including violence, racism, extremism grooming and sexual exploitation from which children and young people need to be protected. At the same time, they must learn to recognise and avoid these risks – to become "internet wise". We need to ensure that they are fully aware of the risks, perform risk assessments and implement a policy for internet use. Pupils need to know how to cope and who to inform if and when they come across inappropriate material.

  Pupils may obtain internet access in Youth Clubs, Libraries, public access points and in homes. Ideally a similar approach to risk assessment and internet safety would be taken in all these locations, although risks do vary with the situation.

- **Responsibility**

  Internet safety depends on Longwill staff, governors, parents and, where appropriate, the pupils themselves taking responsibility for the use of internet and other communication technologies such as mobile phones and iPads or any other mobile device. The balance between educating pupils to take a responsible approach and the use of regulation and technical solutions must be judged carefully.

  This heavily links to out Rights Respecting ethos. In particular, pupils' right to collect information from the media, whilst at the same time be protected from information that may harm them (CRC Article 17) and the right to be protected from being hurt or badly treated (CRC Article 19). These help to develop pupils' own awareness that they have a responsibility to keep themselves and others safe.

- **Reviewing and Monitoring**

  The use of technology has immense benefits but also brings with it the possibility of misuse, which requires close monitoring and supervision. In some cases, access within school must simply be denied, for instance un-moderated chat rooms present immediate dangers and are banned. Fair rules, clarified by discussion and prominently displayed at the point of access will help pupils make responsible decisions.

- **Appropriate Strategies**

  This document describes strategies to help to ensure responsible and safe use. They are based on limiting access, developing responsibility and on guiding pupils towards educational activities. Strategies must be selected to suit our particular school situation and their effectiveness monitored. There are no straightforward or totally effective solutions and staff, parents and the pupils themselves must remain vigilant.

Longwill E-Safety Policy

This E-Safety Policy relates to other policies including those for Computing, Safeguarding, Safe Practice, Behaviour, Acceptable Use for both adults and children, and to the RPSHE policy. Our E-Safety Policy has been written by the school, based upon the KGfL model, the Birmingham BGfL policy and government guidance. It will be reviewed tri-annually.

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 high-quality internet access as part of their learning experience.
- Internet use is a part of the statutory curriculum and a necessary learning tool for staff and pupils.

Internet use will enhance and extend learning

- The school internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
- Clear boundaries will be set for the appropriate use of the internet and digital communications and discussed with staff and pupils. Each child is required to agree to a child-friendly acceptable use policy whenever they log-on to the school system.

- Pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.

Pupils will be taught how to evaluate internet content

- Schools should ensure that the use of internet derived materials by staff and by pupils complies with copyright law.
- Older pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using internet material in their own work.

Why is internet use important?

- The purpose of internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information and business administration systems.
- Internet access is an entitlement for pupils who show a responsible and mature approach to its use.

How does the internet benefit education?

- To keep themselves safe and know what to do if exposed to inappropriate content
- Access to world-wide educational resources including museums and art galleries
- Educational and cultural exchanges between pupils world-wide
- Cultural, vocational, social and leisure use in libraries, clubs and at home
- Access to experts in many fields for pupils and staff
- Facilitates remote learning when required, this has been especially beneficial during COVID to communicate with parents and careers about their child's learning
- Staff professional development through access to national developments, educational materials and good curriculum practice
- Communication with support services, professional associations and colleagues
- Improved access to technical support including remote management of networks;
- Exchange of curriculum and administration data with the LA and at a national level.

How will internet use enhance learning?

- Pupils will be taught what internet use is acceptable and what is not and given clear objectives for internet use.
- Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of pupils.
- Staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity.
- Pupils at Key Stage Two will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation and critical thinking in order that they become 'digitally literate'.

Managing Internet Access

Information system security

- School ICT system security is reviewed regularly.
- Virus protection is installed and updated regularly. Files held on the school's network will be regularly checked.
- Personal data sent over the internet will be encrypted or otherwise secured.

- Use of data storage clouds such as Dropbox, where data is stored outside of the EU is not permitted within school to ensure that data is protected within the regulations of EU law.
- Use of portable media such memory sticks and external hard-drives is not permitted.
- Unapproved system utilities and executable files will not be allowed in pupils' work areas or attached to email.
- Access by wireless devices must be proactively managed and secured with a minimum of WPA2 encryption
- Unapproved software will not be allowed in work areas or attached to email.

E-mail

- Students may only use approved email accounts on the school system.
- Students must immediately tell a teacher if they receive offensive email.
- In email communication, pupils must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.
- Incoming email should be treated with caution and attachments not opened unless the author is known.
- At KS1, access to the internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials.
- Pupils at KS2 will be provided with supervised internet access
- The forwarding of chain letters is not permitted.
- Pupils may not upload photos onto the internet. This should only be done by staff.
- Pupils should be taught never to arrange to meet anyone through the internet.

Published content and the school website

- Staff or pupil personal contact information will not be published. The contact details given online should be the school office.
- The head teacher and DHT will take overall editorial responsibility for online content published by the school and will ensure that content published is accurate and appropriate.
- The school website will comply with the school's guidelines for publications including respect for intellectual property rights, privacy policies and copyright.
- All users must be aware that they should 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, breach any LA/School policies e.g. gambling, do anything which exposes children to danger or any other information which may be offensive to colleagues.

Publishing pupils' images and work

- Photographs or video clips that include pupils will be selected carefully.
- Pupils' full names will not be used anywhere on a school website or other on-line space.
- Pupils' names will not be used in association with their photographs.
- Staff or pupils' home information will not be published.
- Written permission from parents or carers is obtained at the start of every academic year re: photographs of pupils published on the school web site.
- Work can only be published with the permission of the pupils and parents/carers.

Social networking and personal publishing

- Filtering blocks access to social networking sites.
- Newsgroups are blocked unless a specific use is approved.

- Pupils' are advised never to give out personal details of any kind which may identify them, their friends or their location.
- Pupils should be advised on security and older pupils are encouraged to set passwords, to deny access to unknown individuals and to block unwanted communications. Pupils should only invite known friends and deny access to others.

Managing filtering

- The school works in partnership with Entrust and EXA ISP to ensure that systems to protect pupils are reviewed and improved.
- If staff or pupils discover an unsuitable site, it must be reported to the e-safety Coordinator/Network Manager and added to the banned domain list.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- Longwill School has Smoothwall software running on the Network. This software has been installed in-line with City and Audit recommendations. Smoothwall monitors both keyboard (in any application) and internet activity. It continually scans for keywords and images which are possible indications of: inappropriate internet usage, pornography, grooming or other child protection issues. The software will store possible breaches in appropriate use on a secure cloud server monitored by Entrust (Formerly Link2ICT). Screen shots are passes to the Head Teacher and Deputy Head Teacher and the senior leader for investigation. The DHT will decide if screen shots are 'false-positives' or need further investigation. It is essential that children within the school are aware that their activities on the internet and school network are monitored in this way. It is the duty of school staff to inform them of this issue.
- There is a system in place for the recording of e-safety incidents over-seen by the DSL and the Head Teacher.

Managing video conferencing and video streaming

- All school video calls between staff, pupils and parents are made via the schools Teams accounts.
- Only staff can initiate a video call.
- Pupils cannot video call each other or initiate a video or audio call to staff.
- Pupils cannot use the text chat feature, except in a supervised class team chat.
- All video calls and chats are logged in the school Office 365 security portal, although any video or audio conversation is not recorded automatically.

Managing technologies

- The senior management team are aware that technologies such as mobile phones and iPads with wireless internet access can bypass school filtering systems and present a new route to undesirable material and communications.
- Staff are trained to use the 'triple click' locking method to ensure pupils remain working on the app they've been given.
- The sending of abusive or inappropriate text messages via mobile phone, iPad or other learning device is forbidden.
- IPads will not be sent home until parents and pupils have signed the Home School Agreement.
- There is a school phone that can be used where contact with a pupil is required.
- Where possible, all contact with school related matters will be carried out only via authorised school devices (e.g. phone/mobile, school email.)
- Personal devices can be used when necessary, as long as the number is withheld (see Remote Learning Policy)

Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018 (The UK's implementation of EU GDPR)

Policy Decisions

Authorising internet access

- All staff and pupils must read and sign the 'Acceptable Use Policy' before using any school ICT resource. The appropriate AUP is displayed every time a member of staff or pupil logs on to the school system.
- The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.
- Parents/carers will be asked to sign and return a consent form.

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. The school cannot accept liability for any material accessed, or any consequences of internet access.
- The school audits the use of technology to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate and effective. The school monitors activity using appropriate software (Smoothwall).
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
- As with drug related issues, there may be occasions when the police or Multi Agency Safeguarding Hub (MASH) must be contacted. Early contact may be made to establish the legal position and discuss strategies.

Handling e-safety complaints

- Complaints of internet misuse will be dealt with by a senior member of staff and/or the Designated Safeguarding Lead.
- Any complaint about staff misuse must be referred to the head teacher.
- Complaints of a safeguarding nature must be dealt with in accordance with the school safeguarding procedures.
- The school will manage e-safety incidents in accordance with the school behaviour policy and safeguarding procedures, where appropriate.
- Parents will be informed of the complaints procedure (See policy).

Cyber bullying

- Cyber bullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Full details are set out in the school's policy on anti-bullying and behaviour.
- There are clear procedures in place to support anyone in the school community affected by cyberbullying.
- All incidents of cyberbullying reported to the school will be recorded.
- There will be clear procedures in place to investigate incidents or allegations of cyberbullying.
- Pupils, staff and parents/carers will be advised to keep a record of the bullying as evidence.
- The school will take steps to identify the bully, where possible and appropriate. This may include examining school system logs, identifying and interviewing possible

witnesses, and contacting the service provider and the police, if necessary.

- Pupils, staff and parents/carers will be required to work with the school to support the approach to cyberbullying and the school's e-Safety ethos.
- Sanctions for those involved in cyberbullying may include:
    - Asking the bully to remove any material deemed to be inappropriate or a service provider may be contacted to remove content if the bully refuses or is unable to delete content.
    - Internet access may be suspended at school for the user for a period of time.
    - Other sanctions for pupils and staff may also be used in accordance to the schools anti-bullying, behaviour policy or Acceptable Use Policy.
    - Parent/carers of pupils will be informed.
    - The Police will be contacted if a criminal offence is suspected.

Community use of the internet

- The school will liaise with parents and multi-agency professionals to establish a common approach to e-safety as appropriate.

Dealing with incidents

- Any suspicions of misuse or inappropriate activity related to child protection or safeguarding should be reported as prescribed in our Safeguarding Policy.
- Any suspicions of other illegal activity should be reported to the DSL and Head Teacher, who should take advice from appropriate persons
- The police will be contacted if a criminal offence is suspected.
- Suspicions of inappropriate, use of information and communication technology should be reported to the DSL and Head Teacher

Communicating E-Safety

Introducing the e-safety policy to pupils

- E-Safety rules will be posted in all rooms where computers are used.
- The Acceptable Use Policy will be displayed on every device at log on and the children will be familiar with the rules.
- Pupils will be informed that network and internet use will be monitored.
- A programme of training in e-safety will be developed, based on the materials, e.g. from CEOP and materials available through the BGfL.
- Pupil voice is incorporated into e-safety policies and curriculum via the e-safety working group.
- Pupils in Year 5 and 6 will be given passwords when logging in.

Staff and the e-Safety policy

- All staff have access to the E-Safety Policy and its importance has been explained.
- Staff are informed that network and internet traffic is monitored and traced to the individual user and workstation. Discretion and professional conduct is essential.
- Staff that manage filtering systems or monitor ICT use will be supervised by senior management and work to clear procedures for reporting issues.
- Staff should understand that phone or online communications with pupils can occasionally lead to misunderstandings or even malicious accusations.
- As with drug related issues, there may be occasions when the police or Multi Agency Safeguarding Hub (MASH) must be contacted. Early contact may be made to establish the legal position and discuss strategies.

Enlisting parents' and carers' support

- Parents' and carers' attention will be drawn to the school E-Safety Policy in newsletters, the school brochure and on the school web site.
- Parents will have access to the CEOP reporting tool (https://www.ceop.police.uk/About-Us/) from the Longwill website.
- Internet issues will be handled sensitively to inform parents without undue alarm.
- A partnership approach with parents will be encouraged. This includes demonstrations, practical sessions, training and suggestions for safe internet use at home via a termly e-safety focussed newsletter.
- Parents are signposted to the NDCS website for safeguarding/e-safety support.
- Advice on filtering systems and educational and leisure activities that include responsible use of the internet will be made available to parents on the website and via workshops and newsletters.
- Interested parents will be referred to organisations such as Parents Online and NDCS website.

The role of the e-safety officer

A named e-safety officer will:

- Co-ordinate all aspects of e-safety in liaison with the Head Teacher, DSL, staff, pupils and ICT technician to ensure a cohesive approach to online safety.
- Devise and communicate the e-safety curriculum and monitor impact.
- Chair the e-safety group.

S.Sheppard
January 2022

Unicef Rights of the Child:
Article 17
You have the right to get information that is important to you and will not damage your well-being.

Pupil Acceptable Use Agreement

This is how we stay safe when we use computers:

- I will ask a teacher if I want to use the computers/tablets
- I will only use activities that a teacher has told or allowed me to use
- I will take care of computers/tablets and other equipment
- I will ask for help from a teacher if I am not sure what to do or if I think I have done something wrong
- I will tell a teacher if I see something that upsets me on the screen
- I know that if I break the rules I might not be allowed to use a computer/tablet

Signed (child):

Longwill School
Bell Hill
Northfield
Birmingham

Dear Parents

Responsible Internet Use

As part of your child's curriculum and the development of computing skills, Longwill School is providing supervised access to the internet. We believe that the effective use of the World Wide Web and e-mail is worthwhile and is an essential skill for children as they grow up in the modern world.

Although there are concerns about pupils having access to undesirable materials, we have taken positive steps to reduce this risk in school. Birmingham City Council operates a filtering system that restricts access to inappropriate materials.

This may not be the case at home and we can provide references to information on safe internet access if you wish. We also have leaflets from national bodies that explain the issues further.

Whilst we try to ensure that suitable restrictions are placed on the ability of children to access inappropriate materials, the School cannot be held responsible for the nature or content of materials accessed through the internet. The School will not be liable for any damages arising from your child's use of the internet facilities.

Should you wish to discuss any aspect of internet please contact school to arrange an appointment.

Yours sincerely

Mrs Alison Carter
Headteacher

References

Childline: www.childline.org.uk

Childnet: www.childnet.com

CEOP: https://www.ceop.police.uk/About-Us/

Click Clever Click Safe Campaign: http://clickcleverclicksafe.direct.gov.uk

Cybermentors: www.cybermentors.org.uk

Digizen: www.digizen.org.uk

Think U Know website: www.thinkuknow.co.uk

Bullying Online **www.bullying.co.uk**
Advice for children, parents and schools

FKBKO - For Kids By Kids Online **www.fkbko.co.uk**
Excellent internet savvy for kids; KS1 to KS3

Kidsmart **www.kidsmart.org.uk**
An internet safety site from Childnet, with low-cost leaflets for parents.

Think U Know? **www.thinkuknow.co.uk/**
Home Office site for pupils and parents explaining internet dangers and how to stay in control.

Safekids **www.safekids.com**
Family guide to making internet safe, fun and productive

RISK ASSESSMENT for E-SAFETY LONGWILL SCHOOL FOR THE DEAF

HAZARDS IDENTIFIED (Task/Activity/Situation/Process /Stressor)	Persons at Risk	RISKS IDENTIFIED	Initial Risk Rating	Existing Controls	Interim Risk Rating	Further Measures to be taken	Residual Risk Rating	Comments
Using the internet in school Risk of exposure to inappropriate material in terms of **Content**	Pupils & Adult users	Risks from: Racist, Hate, Violent Exploitative Bullying websites Blogs (www.youtube.com) Extremist or Radicalised		BGFL Filters PCE v6 E-Safety Policy and Guidelines Twilight inset Planned intent usage No surfing Explicit teaching of 'internet wise' skills Internet safety rules Acceptable Use Policy	LOW			
Using the internet in school Risk of exposure to inappropriate material in terms of **Contact**	Pupils & Adult users	Risks from: Bullying emails or texts Grooming Blogs Radicalisation Extremism		BGfL filters PCE v6 Anti Bullying Policy Behaviour Policy RPSHE policy Internet safety rules E-Safety Policy No chatroom access Child-friendly search-engines (e.g. Kiddle)	LOW			
Using the internet in school Risk of exposure to inappropriate material in terms of **Commerce**	Pupils	Risks from: Advertising Pupil inability to discern truth from advertising		BGfL filters PCE v6 RPSHE Internet safety rules	LOW			
Using email in school	Pupils & Adult users	Risk of inappropriate **email** content/usage		BGfL Filters Teach children to report issues Email unit at KS2 E-Safety Policy	LOW	Replace usernames with numbers		
School website	Pupils	Risk of identifying pupils		Pupils will not be named. Parents agreement sought No names, addresses used	LOW			

Name of Assessor(s) Alison Carter Signatures(s) _____ Date of Assessment: 5.10.21

Name of Manager: _____ Signatures(s) _____ Date for Review: 5.10.22