Longwill
a primary school for Deaf children

Acceptable Use Policy

September 2021

Staff covered by this procedure:	Staff in schools
Date:	October 2021
Next review date:	12 months from last approval

ACCEPTABLE USE POLICY

The UN CRC identifies that children have a right to information and adults must ensure that it is not harmful to them (Article 17).

The Acceptable Use Policy:

All adults working with ICT equipment in Birmingham schools must ensure that they have read and agree to abide by the Birmingham County Council Acceptable User Policy.

Effective communication across the school community is key to achieving the school vision for safe and responsible citizens. To achieve this we will:

- Make this policy, and related documents, available on the school website at www.longwill.bham.sch.uk
- Introduce this policy, and related documents, to all stakeholders at appropriate times. This will be at least once a year or whenever it is updated
- Post relevant e-Safety information in all areas where computers are used
- Provide e-Safety information at parents meetings, review meetings, on the website and through the school newsletter

The Head and Governors have ultimate responsibility for establishing safe practice and managing e-Safety issues at our school. The role of e-Safety lead is allocated to the computing lead and is part of a wider e-Safety team including governors and senior leadership team. They are the central point of contact for all e-Safety issues and will be responsible for day to day management. All members of the school community have certain core responsibilities within and outside the school environment. They should:

- Use technology responsibly
- Accept responsibility for their use of technology
- Model best practice when using technology
- Report any incidents to the e-Safety lead using the school procedures
- Understand that network activity and online communications are monitored, including any personal and private communications made via the school network
- Be aware that in certain circumstances where acceptable use is suspected, the person responsible will be accountable for their actions and disciplinary procedures may be instigated.

Physical Environment / Security

The school provides a safe environment for the whole community and we review both physical and network security regularly and monitor who has access to the system consulting with the LA where appropriate.

- Anti-virus software is installed on all computers and updated regularly
- Staff with school laptops & iPads must bring in them in every month for anti-virus software to be updated by our school technician

- Central filtering is provided and managed by Link2ICT. All staff and students understand that if an inappropriate site is discovered it must be reported to the e-Safety lead who will report it to the Link2ICT Service Desk to be blocked. All incidents will be recorded in the e-Safety log for audit purposes. **Do not print or share electronically with anyone.**
- Requests for changes to the filtering will be directed to the e-Safety lead in the first instance. Change requests will be recorded in the e-Safety log for audit purposes
- The school uses Smoothwall on all school owned equipment to ensure compliance with the Acceptable Use Policies. Pupils and staff use is monitored by HT and named senior staff.
- All staff are issued with their own username and password for network access. Visitors/supply staff are issued with temporary IDs.
- Pupils have their own username and password and understand that this must not be shared

Mobile / emerging technologies

- Teaching staff at the school are provided, where possible, with a laptop or ipads for educational use and their own professional development. All staff understand that the Acceptable Use Policies apply to this equipment at all times
- To ensure the security of the school systems, personal equipment is currently not permitted to be connected to the school network
- Staff understand that they should use their own mobile phones sensibly and in line with school policy. Mobile phones should not be on your person during school time
- Pupils should not bring mobile phones to school
- The Education and Inspections Act 2006 grants the Head the legal power to confiscate mobile devices where there is reasonable suspicion of misuse and the Head will exercise this right at their discretion
- Picture/videos of staff and pupils should not be taken on personal devices
- New technologies are evaluated and risk assessed for their educational benefits before they are introduced to the school community

School iPads

iPad - Data Protection and Security

- All school staff must have their iPad enrolled into the schools 'Mobile Device Management' system. At no point should a member of staff attempt to remove their device from this system.
- All Longwill school devices are managed by the IT team. Do not try to manage your staff device yourself via iTunes or any other management software.
- Longwill school provides paid for apps via a managed Apple ID. Do not use your personal Apple ID on the device.

- Do not set up your personal email address on a school iPad.
- Do not link up personal third party apps or services, such as Dropbox or other storage; on-demand TV; other media streaming services.
- Do not to sign into your personal social media accounts, e.g., Twitter; Facebook; LinkedIn.
- You must not jailbreak your device, or otherwise hack, or tamper with it.

iPad - User Responsibility

- Your iPad device must be in the provided protective case at all times.
- Handle your device with care and respect. Do not throw, damage, place heavy items on, or intentionally drop your device.
- Only approved cleaning materials can be used to clean your device, such as laptop or tablet sprays and cloths.
- Do not keep, or leave your iPad unattended in vehicles.
- Keep your iPad safe and secure at all times. You should know where your iPad is at all times.
- Ensure your battery is charged, and ready for school use each and every morning.

iPad - Lost, Damaged, or Stolen Devices

- If your device becomes lost or stolen, report it to Alison Carter or Chris Ward as a matter of urgency.
- If your device has become damaged, report it to Chris Ward, Martin Belton or Louise Taggart, and hand over the device to them.
- You must not carry out repairs on any school-owned device.
- You must not solicit any individual or company to repair a school-owned device on your behalf.

iPad - Safeguarding and E-Safety

- All device usage is subject to the rules and guidelines of the school's E-Safety policy and the acceptable use policy. Anyone in breach of this policy may be subject, but not limited to disciplinary action, confiscation, removal of content, or referral to external agencies.

- Do not tamper with iPad devices belonging to other members of staff. Anyone found trying to access another staff member's device or associated content will be subject to disciplinary action.

- If an iPad is found, return it immediately to Chris Ward, Martin Belton or Louise Taggart.

- As with all other school devices, outlined within our ICT and Safeguarding policies, you are strictly forbidden from using your device to create, store, access, view, download, distribute, send, upload inappropriate content or materials.

- You are forbidden from utilising your iPad to partake in illegal activities of any kind.

- Do not use your iPad to post images, movies, or audio to a public facing part of the internet, without the express permission of all individuals imaged/recorded. Where this includes students, refer to the head teacher, and ensure that full permission has been received from the head, as well as parents/guardians before a post is made.

- Your iPad and any content are subject to routine and ad-hoc monitoring by a member of the IT team. You must hand over your device upon request by any senior member of staff.

- You must ensure compliance with the E-Safety policy and the acceptable use policy when using your iPad.

iPad - Personal Use

- Your iPad device is not permitted for personal use. It has been provided for work-related use only.

- Refer to the schools E-Safety policy and acceptable use policy for guidelines on utilising your iPad device to browse the internet outside of Longwill school.

- Do not grant access to anyone outside of Longwill school, unless expressly authorised to do so by a member of the senior management team.

- Staff are prohibited from taking or storing personal photos/videos on school devices as these may be seen in school by pupils or other staff.

Published content

The Head and Deputy Head take responsibility for content published to the school web site. Class teachers and phase leaders are responsible for the editorial control of work published by their pupils

- The school will hold the copyright for any material published on the school web site or will obtain permission from the copyright holder prior to publishing with appropriate attribution

- The school encourages the use of e-mail for contact via the school office/generic e-mail /staff e-mail addresses

- The school does not publish any contact details for the pupils

Guidance for staff personal use:

- Do not give anyone access to your login name or password.
- USB sticks should not be used for school business at any time.
- Do not open other people's files without express permission.
- Do not release personal details including phone numbers, or personal e-mail addresses of any colleague or pupil over the internet.
- Do not reproduce copyright materials without first getting permission from the owner. Many people will make their work freely available for education on request. Acknowledge sources on all resources used.
- Do not attempt to visit sites which might be considered inappropriate. All internet use is monitored and logged. Downloading some material is illegal and the police or other authorities may be called to investigate such use.
- Use of school internet access for business, profit, advertising or political purposes is strictly forbidden.
- Users should log out and close their browser when their session has finished.

Personal E-mail

- Follow school guidelines contained in the Computing policy for the use of e-mail.
- Observe *netiquette* on all occasions. E-mail should not be considered a private medium of communication.
- Do not include offensive or abusive language in your messages or any language which could be considered defamatory, obscene, menacing or illegal. Do not use language that could be calculated to incite hatred against any ethnic, religious or other minority.
- Make sure nothing in the messages could be interpreted as libellous.
- Do not send any message, which is likely to cause annoyance, inconvenience or needless anxiety.
- Do not send any unsolicited promotional or advertising material nor any chain letters or pyramid selling schemes.

When using the Internet, Virtual Learning Environment or e-mail with children

- Remind children of the rules for using the internet, VLE or e-mail.
- Watch for accidental access to inappropriate materials and report the offending site to the helpdesk – schoolshelpline@birmingham.gov.uk.
- Check before publishing children's work; make sure that you have parental permission.
- Ensure children are not named in photographs.
- Report any breaches of the school's Internet Policy to the headteacher.

Photographs and digital video

- Where possible, school cameras should be used and digital photos taken should stay in school.

Responding to incidents

Inappropriate use of the school resources will be dealt with in line with other school policies e.g. Behaviour, Anti-Bullying and Safeguarding Policy or a range of other policies and processes.

- Any suspected illegal activity will be reported to the HT in the first instance. Other agencies may be contacted.
- Third party complaints, or from parents concerning activity that occurs outside the normal school day, should be referred directly to the Headteacher.
- Breaches of this policy by staff will be investigated by the Headteacher.
- Action will be taken under Birmingham City Council's Disciplinary Policy where a breach of professional conduct is identified.
- All monitoring of staff will be carried out by a least 2 senior members of staff.
- Pupil breaches relating to bullying, drugs misuse, abuse and suicide must be reported to the nominated child protection representative and action taken in line with school anti-bullying and safeguarding / child protection policies. There may be occasions when the police must be involved.
- Serious breaches of this policy by pupils will be treated as any other serious breach of conduct in line with school Behaviour Policy.
- For all serious breaches, the incident will be fully investigated, and appropriate records made on personal files with the ultimate sanction of exclusion reserved for the most serious of cases
- Minor offences by pupils, such as being off-task visiting games or email websites will be handled by the teacher in situ by invoking the school behaviour policy
- The Educations and Inspections Act 2006 grants the Head the legal power to take action against incidents affecting the school that occur outside the normal school day and this right will be exercised where it is considered appropriate

AJ/AC

October 2021

Longwill
a primary school for Deaf children

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): .....

Note 1

Inappropriate websites are those categorised as:

- Alcohol (al)

  This category includes URLs that sell, promote, or advocate the use of alcoholic beverages, including beer, wine, and hard liquors.

- Anonymizers (an)

  This category includes URLs that enable anonymous Web browsing through an intermediary to prevent unauthorized parties from gathering personal information, but also allow users access to any Web page and bypass blocking software. Pages that provide free proxy IP addresses are also included in this category.

- Anonymizing Utilities (au)

  This category includes Web page language translators and Web-page-caching utilities that could be used as anonymizers, without the express purpose of bypassing filtering software.

- Chat (ch)

  This category includes sites that provide social posting and receiving of real-time messages. This includes public or private chat rooms and chat software downloads such as IRC that allow twoway messaging.

- Criminal Skills (cs)

  This category includes URLs that either provide instructions for or identify methods to promote, encourage, or provide the skills to commit illegal or criminal activities. These include bomb-making, phreaking (breaching phone security or phone service theft), consumer scams and fraud, terrorism, evading law enforcement, stalking, lock picking, passing urine tests and selling pirated material, commercial software, music, videos, or fake IDs.

- Drugs (dr)

  Sites in this category provide information on the purchase, manufacture, and use of illegal or recreational drugs. This includes displaying, selling, or detailing the use of drug paraphernalia, as well as tips on legal highs, such as glue sniffing, the misuse of prescription drugs, or the abuse of other legal substances.

- Extreme (ex)

  This category is used in conjunction with Gruesome Content, Hate Speech, Politics/Opinion, Pornography, Violence, or Game/Cartoon Violence to identify URLs that are at the outer limits of these categories, being gory, perverse, or horrific in nature. An example is child pornography, which would have both the Pornography and Extreme categorization.

- Gambling (gb)

  This category includes sites that allow users to wager or place bets online or provide gambling software that allows online betting i.e. casino games, betting pools, sports betting etc.

- Gruesome Content(tg)

  This category includes URLs with content such as tasteless humor, excretory functions (vomiting, urinating, or defecating), graphic medical or accident scene photos (containing blood or wounds), and some extreme forms of body modification (cutting, branding, or genital piercing).

- Hacking (hk)

  This category includes URLs that distribute information and hacking tools (root kits, kiddy scripts, etc.) that help individuals gain unauthorized access to computer systems.

- Hate Speech (hs)

  This category is dedicated to any sort of information that would encourage the oppression of a specific group of individuals. This includes promoting, explicitly or implicitly, an agenda against groups based on race, religion, nationality, gender, age, disability, or sexual orientation.

- Malicious Sites (ms)

  Sites in this category deploy code that has been designed specifically to hijack your computer's settings or activity.

- P2P/File Sharing (pn) Soon available on all platforms*

This category includes the exchange of files between computers and users for business or personal use. An example of P2P use is downloadable, shared music. P2P clients allow users to search for and exchange files from a peer-user network. They often include SpyWare or real-time chat capabilities. P2P may offer bandwidth usage risks, or allow users to compromise network security by distributing proprietary or sensitive data outside a secured network.

- Phishing (ph) Soon available on all platforms*

  This category includes sites that typically arrive in hoax e-mail established only to steal users' account information. These sites falsely represent themselves as legitimate company Web sites in order to deceive and obtain user account information that can be used to perpetrate fraud or theft.

- Pornography (sx)

  This category includes URLs that contain materials that are intended to be sexually arousing or erotic. This includes fetish pages, animation, cartoons, stories, and child pornography.

- Profanity (pr)

  This category includes URLs that contain crude, vulgar, or obscene language or gestures.

- Remote Access (ra)

  Sites in this category provide information about gaining remote access to a program, online service or an entire computer system. While often used legitimately by people who want to use their computer from a remote location, it also creates a potential security risk. Backdoor access is often written by the original programmer.

- Spam Email URLs (su) Soon available on all platforms*

  This category includes URLs that arrive in unsolicited SPAM emails. These are harvested directly from user's email inboxes.

- Spyware (sy)

  This category includes URLs that download software that covertly gathers user information through the user's Internet connection, without his or her knowledge, usually for advertising purposes. This may be considered a violation of privacy and may have bandwidth and security implications. These practices are not part of the normal practice of software registration. This category is mainly populated using expert 3rd party information.

- Tobacco (tb)

  This category includes URLs that sell, promote, or advocate the use of tobacco products, including cigarettes, cigars, and pipe and chewing tobacco.

- Usenet news (na)

  The Usenet News category includes URLs that provide Web access to Usenet news groups and archives of files uploaded to newsgroups.

- Violence (vi)

  The violence category includes real or lifelike images or text that portray, describe, or advocate physical assaults against humans, animals, or institutions (for example: depictions of war, suicide, mutilation, dismemberment). Sites showing the outer end of this spectrum, such as depictions of torture, gore, or horrific death, are also rated as Extreme.

- Weapons (we)

  This category includes URLs that provide information about buying, making, modifying, or using weapons such as guns, knives, swords, as well as ammunition or explosives. Weapons pages may highlight personal or military use.

Birmingham City Council Internet Use Policy, Internet Use Code of Practice and Email Use Policy (Linked from www.bgfl.org/esafety)