Longwill
a primary school for Deaf children

ACCEPTABLE USE POLICY

September 2015

ACCEPTABLE USE POLICY

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 evenings, information meetings 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 co-ordinator is been allocated to the deputy headteacher. 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 co-ordinator 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 endeavours to provide 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 must bring in their laptops 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 co-ordinator 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

- Requests for changes to the filtering will be directed to the e-Safety co-ordinator in the first instance. Change requests will be recorded in the e-Safety log for audit purposes
- The school uses Policy Central Enterprise 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
- All pupils are issued with 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
- 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

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 students

- 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 to contact the school 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.
- Do not introduce usbs into the system without first having them checked for viruses.
- Sticks should always be encrypted.

- Do not open other people's files without express permission. Do not corrupt, interfere with or destroy any other user's information.
- Do not release personal details including phone numbers, fax 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 (note 1). 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 ICT 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 or telephone 0121 303 5210
- 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 designated person.

Photographs and digital video

- Where possible, school cameras should be used and digital photos taken should stay in school.
- It is recognised that from time to time images will be taken home by staff to work on for educational purposes. All staff should take all reasonable measures to keep them secure.

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 Child Protection Policy.

- Any suspected illegal activity will be reported directly to the police. The Link2ICT Service Desk will also be informed to ensure that the Local Authority can provide appropriate support for the school
- Third party complaints, or from parents concerning activity that occurs outside the normal school day, should be referred directly to the Head
- 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.
- Incidents will be fully investigated and appropriate records made on personal files with the ultimate sanction of summary dismissal reserved for the most serious of cases involving gross misconduct.
- 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 inline with school anti-bullying and 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 inline 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 student offences, 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

AC
September 2015

I have read and understand the Acceptable Use Policy.

Signed:

Print:

Position:

Date:

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)