LONGHILL

HIGH SCHOOL

Acceptable Use Policy

Lead Author:	Jimmy Hollingworth, Business Manager

Acceptable Use Policy August 2023

SLT (I:), Policy Library, Longhill High School Policies

STAFF POLICIES:

1. Acceptable use of ICT

Equipment Principles

Longhill High School is committed to safeguarding its ICT infrastructure to ensure it can be used in the most effective manner to support teaching and learning and all necessary administrative processes. Ensuring the safety and integrity of the school ICT infrastructure is the responsibility of all staff.

The school encourages staff to fully use the ICT infrastructure and to make use of available portable ICT equipment offsite to support them in their work. The school encourages this use in a responsible and professional manner. Portable computers include for example laptops, tablets and other portable ICT devices where provided.

As a user of ICT services of the school you have a right to use its computing services; that right places responsibilities on you as a user which are outlined below. If you misuse school computing facilities in a way that constitutes a breach or disregard of this policy, consequences associated with that breach may apply to you, and you may also be in breach of other school regulations.

Ignorance of this policy and the responsibilities it places on you is not an excuse in any situation where it is assessed that you have breached the policy and its requirements.

Staff are advised of this policy during their induction and of the requirement for them to adhere to the conditions therein.

For the purposes of this policy the term "computing services" refers to any ICT resource made available to you, any of the network services, applications or software products that you are provided access to and the network/data transport infrastructure that you use to access any of the services (including access to the internet). Staff who connect their own ICT to the school network and the services available (where permitted) are particularly reminded that such use requires compliance to this policy.

Purposes

- To protect the school networks and equipment
- To protect the school data
- To protect the school and its employees from activities that might expose them to legal action from other parties

Guidelines

Password Security

Access to systems and services is controlled by a central computing account and password. Staff are allocated their User ID and initial password as part of their induction with the school.

Access and continued use of your user account is conditional on your compliance with this policy. User IDs and passwords are not to be shared or revealed to any other party. Those who use another person's user credentials and those who share such credentials with others will be in breach of this policy.

Initial default passwords issued to any user should be changed immediately following notification of account set up. Passwords should be routinely changed (every 3 months is recommended) and should be changed immediately if the user believes or suspects that their account has been compromised. Management and IT support should also be notified if a compromise takes place or is in any way suspected.

General Conditions

In general, use of school "computing services" should be for your study, research, teaching or the administrative purposes of the school. Modest use of the facilities and services for personal use is accepted so long as such activity does not contravene the conditions of this policy.

- Your use of the school computing services must at all times comply with the law.
- Your use of the school computing services must not interfere with any others' use of these facilities and services.
- You are not entitled to use a computer that you have not been authorised to use.
- You must not access any program or data which has not been specifically authorised for your use.
- You must not use or copy any data or program belonging to other users without their express and specific permission.
- You must not alter computer material belonging to another user without the users' permission.
- You must not use school computing services to harass, defame, libel, slander, intimidate, impersonate or otherwise abuse another person.
- You must not use school computing services for the creation, collection, storage, downloading or displaying of any offensive, obscene, indecent or menacing images, data or material capable of being resolved into such. (There may be certain legitimate exceptions for educational purposes which would require the fullest disclosure and special authorisation from the Head).
- You must not use the school computing services to conduct any form of commercial activity without express permission.
- You must not use the school computing services to disseminate mass (unsolicited) mailings.
- You must not install, use or distribute software for which you do not have a licence, and which is not first authorised by the ICT Department for installation.
- You must not use any peer-to-peer file sharing software without the express written permission of the ICT manager.
- You must not use any IRC or messenger software including, but not limited to AOL, MSN, Yahoo! or other "Messengers", IRC or "chat" clients unless expressly authorized to do so for work related purposes.
- You must not use any form of network monitoring which will intercept data not specifically intended for you unless this activity is a part of your normal job responsibilities or has been specifically authorised by the Headteacher/Governing Body

This policy aims to provide a summary of the guidelines for staff, but is by no means exhaustive. In adhering to the spirit of this document as well as the rules herein, staff will be able to use the network at Longhill High School in a safe and responsible way.

This policy refers to, and complies with, the following legislation and guidance:

- Data Protection Act 2018

- The UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2020
- Computer Misuse Act 1990
- Human Rights Act 1998
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Education Act 2011
- Freedom of Information Act 2000
- Education and Inspections Act 2006
- Keeping Children Safe in Education 2023
- Searching, screening and confiscation: advice for schools 2022
- National Cyber Security Centre (NCSC): Cyber Security for Schools
- Education and Training (Welfare of Children) Act 2021
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Meeting digital and technology standards in schools and colleges

Data Security

The school holds a variety of sensitive data including personal information about students and staff. If you have been given access to this information, you are reminded of your responsibilities under data protection law.

You should only take a copy of data outside the school systems if absolutely necessary, and you should exhaust all other options before doing so. This includes putting sensitive data onto laptops, memory sticks, cds/dvds, and any portable media or into emails. If you do need to take data outside the school, this should only be with the authorisation of the school Data Protection Officer. As part of this you should perform a risk assessment on the implications of it falling into the wrong hands, and take appropriate steps to mitigate against this. This will almost certainly include encrypting the information, and checking the data protection statements of any recipients of the data.

There are a variety of methods of remote access to systems available (in particular using VPN and remote desktop or terminal services) which allow you to work on data in-situ rather than taking it outside the school, and these should always be used in preference to taking data off-site. Use of any remote access software and/environments must comply in all cases with the conditions outlined in this policy.

The ICT Department offers a variety of information and support to help you keep data secure. If you are uncertain about any aspect of data security, you must contact them or your Data Protection Officer for advice.

Anti-Virus and Firewall Security

All personal computers are installed with current versions of virus protection and firewall software (where necessary) by the ICT Department. Users are not to alter the configuration of this software unless express permission has been obtained from the ICT Department. This software is installed to prevent an attack from malicious software and to prevent loss of data and corruption of programs/files.

Users must ensure that they are running with adequate and up-to-date anti-virus software at all times. If any user suspects viral infection on their machine, they should inform the ICT Department immediately. If the ICT Department detects a machine behaving abnormally due to a possible viral infection it will disconnected from the network until deemed safe, and must remain unused until reinstated by the IT support staff.

Physical Security

The users of ICT equipment should always adhere to the following guidelines:

- Treat equipment safely, in the same manner as a reasonable person would
- Keep liquids away from ICT equipment
- Do not place heavy objects on ICT equipment
- Do not drop ICT equipment or objects onto it
- Any portable computer must be securely locked away when not in use.
- Portable computer security is your responsibility at all times.
- Do not leave the portable computer unattended in a public place or within the school
- Do not leave the portable computer on view inside your car. It should be locked away in your car out of sight.
- Extra reasonable care must be taken to prevent the loss of any portable media which contain confidential school data, and any portable data storage devices must be encrypted. Encryption is the responsibility of the end user, not the ICT support staff.
- Staff supervising students using ICT equipment should ensure students take reasonable care of such equipment.

Remote Access

Remote access to the school network is possible where this has been granted by the ICT Department.

Remote connections are considered direct connections to the school network. As such, generally accessing services remotely, subjects the user to the same conditions, requirements and responsibilities of this policy.

All connection attempts are logged.

Monitoring and Logging

Activities regarding network transactions may be monitored and logged and kept for an appropriate amount of time. Logs are taken for reasons of security, diagnostic and account/audit reasons. Logs are available only to authorised systems personnel and kept for no longer than necessary and in line with current data protection guidelines.

Such records and information are sometimes required - under law - by external agencies and authorities. The school will comply with such requests when formally submitted.

Breaches of This Policy

Incidents which are determined to be in contravention of this policy will be assessed for their severity. Investigating such incidents may require the collection and evaluation of user related activity and evidence.

It is not possible to provide an exhaustive list of potential ways in which a user may contravene this policy but in general such breaches will be categorised into one of three levels of severity and each level of breach will carry with it a possible range of sanctions, consequences and/or penalties.

In the event a portable computer is damaged or lost as a result of non-compliance with this policy or as a result of other negligent action, then you may be required to make a full or partial contribution towards any reparation/replacement costs, at the discretion of the school.

Minor Breach

This level of breach will attract a verbal warning which will be held recorded for 12 months. In general this category will relate to behaviour or misuse of computer facilities that can be characterised as disruptive or a nuisance. Examples of this level of non-compliance would include:

- Taking food and/or drink into ICT facilities where they are forbidden.
- Sending nuisance (non-offensive) email
- Behaving in a disruptive manner.

Not all first offences will be automatically be categorised at this level since some may be of a significant or impact that elevates them to one of the higher levels of severity.

Moderate Breach

This level of breach will attract more substantial sanctions and/or penalties. Examples of this level of non-compliance would include:

- Repeated minor breaches within the above detailed 12 month period.
- Unauthorised access through the use of another user's credentials (username and password) or using a computer in an unauthorised area.
- Assisting or encouraging unauthorised access.
- Sending abusive, harassing, offensive or intimidating email.
- Maligning, defaming, slandering or libelling another person.
- Misuse of software or software licence infringement.
- Copyright infringement.
- Interference with workstation or computer configuration.

Severe Breach

This level of breach will attract more stringent sanctions, penalties and consequences than those above, and access to computing facilities and services may be withdrawn (account suspension) until the disciplinary process and its outcomes have been concluded. Examples of this level of breach would include:

- Repeat moderate breaches.
- Theft, vandalism or wilful damage of/to ICT facilities, services and resources.
- Forging email i.e. masquerading as another person.
- Loading, viewing, storing or distributing pornographic or other offensive material.
- Unauthorised copying, storage or distribution of software.

- Any action, whilst using school computing services and facilities deemed likely to bring the school into disrepute.
- Attempting unauthorised access to a remote system.
- Attempting to jeopardise, damage circumvent or destroy ICT systems security.
- Attempting to modify, damage or destroy another authorised user's data.
- Disruption of network communication capability or integrity through denial of service attacks, port scanning, monitoring, packet spoofing or network flooding activities.

Process

An investigation will be carried out, in confidence, by school leadership under the direction of the Headteacher. That investigative report will be passed to the staff member's Line Manager, to be considered within the school disciplinary procedures. Each set of disciplinary procedures provide for an appeal stage.

2. Use of telephones, email and internet by staff

Principles

The provisions of this Policy apply to all members of staff, whether or not they have access to, or sole use of, a telephone or e-mail/the Internet on a personal computer. Although access to such facilities does not form part of the benefits provided to staff, it is recognised that there are occasions when employees might legitimately make private use of these facilities. This policy is intended to make clear what constitutes legitimate use. It is intended not to place employees under unjustifiable scrutiny, but to give them a high measure of security and confidence about their use of e-mail, telephones and the internet.

The sections of the policy covered by misconduct and misuse should be read in conjunction with the appropriate staff disciplinary procedure.

This policy has been designed to safeguard the legal rights of members of staff under the terms of both the Data Protection Act and the Human Rights Act.

Purposes

To provide guidance on inappropriate use of school telephones, email and internet facilities. To clarify when the school may monitor staff usage of these facilities.

Guidelines

Use of telephones

There will be occasions when employees need to make short, personal telephone calls on school telephones in order to deal with occasional and urgent personal matters. Where possible, such calls should be made and received outside the employee's normal working hours or when they do not interfere with work requirements.

The use of school telephones for private purposes, which are unreasonably excessive or for school purposes which are defamatory, obscene or otherwise inappropriate, may be treated as gross misconduct under the appropriate disciplinary procedure.

Where the school has grounds to suspect possible misuse of its telephones, it reserves the right to audit the destination and length of out-going calls and the source and length of in-coming calls. This would not normally involve the surveillance of calls but in certain rare circumstances where there are reasonable grounds to suspect serious misconduct, the school reserves the right to record calls.

Use of email

As with telephones it is recognised that employees can use e-mail for personal means in the same manner as that set out for telephones above. E-mail should be treated like any other form of written communication and, as such, what is normally regarded as unacceptable in a letter or memorandum is equally unacceptable in an e-mail communication.

Employees should be careful that before they open any attachment to a personal e-mail they receive, they are reasonably confident that the content is in no sense a risk to security, obscene or defamatory to avoid contravening the law. Equally, if an employee receives an obscene, compromised in terms of security, or defamatory e-mail, whether unwittingly or otherwise and from whatever source, s/he should not intentionally forward the e-mail to any other address, unless specifically requested to do so by an investigator appointed by the school. Any suspicious attachments to email or indeed any website or software which requests login details should not be used until verified safe by the ICT support department. Any other use of e-mail for either personal or school purposes to send or forward messages or attachments which are in any way defamatory, obscene or otherwise inappropriate will be treated as gross misconduct under the appropriate disciplinary procedure.

Where the school has reasonable grounds to suspect misuse of e-mail in either scale of use, content or nature of messages, it reserves the right to audit the destination, source and content of e-mail to and from a particular address.

The school also reserves the right to access an employee’s e-mail account in her/his unexpected or prolonged absence (e.g. due to sickness) in order to allow it to continue to undertake the employee’s normal role. In normal circumstances the employee concerned will be contacted before this is done, in order to provide him/her with prior knowledge.

Use of the Internet

The primary reason for the provision of internet access is for the easy retrieval of information for educational purposes, or to make use of learning resources, or to make legitimate authorised purchases to enhance the ability of its staff to undertake their school role. However, it is legitimate for employees to make use of the internet in its various forms in the same way as email above as long as it is not used to view or distribute improper material such as text, messages or images which are derogatory, defamatory or obscene.

Unauthorised use of the internet, which is unreasonably excessive for personal use or for purposes which are defamatory, obscene or otherwise inappropriate will be treated as gross misconduct under the appropriate disciplinary procedure. The school reserves the right to audit the use of the internet from particular personal computers or accounts where it suspects misuse of the facility.

Monitoring the use of telephone, e-mail and the Internet.

It is not school policy, as a matter of routine, to monitor an employee’s use of the school telephone or e-mail service or of the internet via the school networks. However, as has been stated, where there are reasonable grounds to suspect an instance of misuse or abuse of any of these services, the Headteacher or Governing Body may grant permission for the auditing of an employee’s telephone calls e-mail or use of the internet. Once approved, the monitoring process will be undertaken by designated staff acting, for operational purposes, under the direction of the Headteacher. These staff are required to observe the strictest confidentiality when undertaking these activities and they will monitor only to the extent necessary to establish the facts of the case. They will make their reports directly to the Headteacher/Governing Body or their delegated representative to enable human resources to advise the appropriate line manager/head of faculty of the actions that may need to be taken in any particular case. When monitoring is approved, the case for continued monitoring shall be reviewed on a regular basis with a view to terminating monitoring in as short a period of time as possible.

3. Safe use of online resources
Principles

This applies wherever access to Longhill High School Management Information Systems (MIS) are provided. This applies to all online/intranet resources provided by Longhill High School, for example Capita SIMS (Bromcom), Classcharts and the Parent Portal Learning Platform. This policy applies whenever information is accessed through a Longhill High School MIS, whether the computer equipment used is owned by Longhill High School or not. The policy applies to all those who make use of Longhill High School MIS resources.

Purposes
Security

- This Policy is intended to minimise security risks. These risks might affect the integrity of Longhill High School data, the authorised MIS user and the individuals to which the MIS data pertains. In particular these risks arise from:
    - The intentional or unintentional disclosure of login credentials
    - The wrongful disclosure of private, sensitive and/or confidential information
    - Exposure of Longhill High School to vicarious liability for information wrongfully disclosed by authorised users.

Data Access

- This policy aims to ensure all relevant aspects of the Data Protection Act (1998) and Fair Processing Policy are adhered to.
- This Policy aims to promote best use of the MIS systems to further the communication and freedom of information between Longhill High School and Parents/Carers.
- In addition, data processing should at all times comply with and be compliant to the conditions of GDPR

Guidelines

The Longhill High School online systems are provided for use only by persons who are legally responsible for student(s) currently attending the school.

Access is granted only on condition that the individual formally agrees to the terms of this and any other relevant policy.

The authorising member of the Longhill High School staff **must** confirm that there is a legitimate entitlement to access information for students the names of whom must be stated on the Online Usage Policy Declaration, where applicable.

A copy of the form will be held by the school for audit purposes.

Personal Devices

Work-use: Some access to email or remote resources from personal devices may be essential to your role at Longhill High School. Where such access is necessary, no Longhill data may be stored locally on personal devices. Users agree to apply the latest operating system and security software updates to ensure the highest levels of device security before accessing remote systems. All systems must be used securely, must not be left logged in and unattended, and must comply with all relevant security and e-safety policies whilst in use. Users must ensure they are logged out of any Longhill High School systems as soon as any work activities are finished.

Non-work use: Personal devices are not banned from Longhill High School, and a positive work/life balance should be encouraged. Excessive use of personal internet/devices throughout the day may be cause for warnings or discipline as outlined elsewhere in this policy. Public Wi-Fi is occasionally made available for staff to use.

Personal Use

Information made available through the MIS system is confidential and protected by law under the Data Protection Act 1998. To that aim:

Users must not distribute or disclose any information obtained from the MIS to any person(s) with the exception of the student to which the information relates or to other adults with parental/carer responsibility.
Best practice is not to access the system in any environment where the security of the information contained may be placed at risk.

Password Policy

Staff must assume personal responsibility for usernames and passwords. Never use anyone else's username or password.

You must always keep your individual user name and password confidential. These usernames and passwords should ***never*** be disclosed to anyone. Passwords and user names should never be shared.

In some instances users may be given the right to change passwords from the one originally issued. These passwords should be changed frequently by all users, and when any breach of secrecy is suspected or proven. IT support or line management should be informed of any such breach. Where passwords are prescribed for users or for services, IT support (or line management or relevant member of staff) should be informed immediately should a change be required or breach occurs. Reminders will be sent to staff in preference of enforcement at this time, though this may be subject to change.

Questions, Complaints and Appeals

MIS users should address any complaints and enquiries about the MIS system to Longhill High School in writing to The Head of ICT Support. Where availability or concerns pertaining to data processing arise, these must be directed to the Data Protection Officer.

Longhill High School reserves the right to revoke or deny access to MIS systems of any individual under the following circumstances:

- The validity of parental/carer responsibility is questioned

• Court ruling preventing access to child or family members is issued

• Users found to be in breach of this policy

If any child protection concerns are raised or disputes occur Longhill High School will revoke access for all parties concerned pending investigation.

Please note: Where MIS access is not available Longhill High School will still make information available according to Data Protection Act (1998) law.

Users are liable for any potential misuse of the system and/or breach of the data protection act that may occur as a result of failing to adhere to any of the rules/guidelines listed in this document.

Software

Software should be purchased or acquired from reputable vendors, in all cases following approval in writing from the Network Manager. Installation of any software (where staff have rights to do so) must be approved in writing by the Network Manager; no software may be installed by staff alone. Breach of this condition represents a large security and data protection risk, and may be grounds for disciplinary action.

Further guidelines

Staff must not:

- create, transmit or cause to be transmitted any threatening material, material which breaches copyright, material likely to cause damage, offend, distress, cause anxiety to or prevent another user from carrying out their duties

- cause a computer or another user of the network to access unauthorised data (secured or unsecured)

- impair the operation of a computer either deliberately or recklessly

- act in a way that would cause or create risk of damage to physical IT systems or data

- create, supply or obtain articles (including but not limited to software and data) for use in the above and following items

- partake in activity defined as Cyber-dependent crimes and/or Cyber-enabled crimes (see CPS http://www.cps.gov.uk/legal/a_to_c/cybercrime/#a23 and CPS http://www.cps.gov.uk/legal/a_to_c/cybercrime/#a24)

- access, store, transmit or possess pornographic, terrorist/extremist, illegal or unprofessional material and/or data relating to the aforementioned

Visitors and volunteers

Whilst it won't be necessary for all visitors and volunteers to sign this/an Acceptable Use Policy, it is important that Longhill High School representatives provide regular visitors and volunteers with clear expectations regarding online behaviour and confidentially. If you arrange for/are responsible for a visitor or volunteers who may need to sign an AUP (either an amended version of this AUP or potentially as a separate document) please do ensure that this is done and the document dated and retained. Visitors who require this may include:

- Governors or trust/committee members
- Parental volunteers
- Visiting IT staff such as mobile technicians
- External speakers or organisations working with children

In some cases, visitors or volunteers may not have accessed any professional training regarding child protection or safe professional practice. This Acceptable Use Policy can therefore help ensure that clear information regarding the settings expectations regarding online conduct is provided; this is especially important to ensure confidentiality policies are respected. For example a concern could arise if a parent volunteer posted comments on social media about another child's behaviour. There will also be situations whereby visitors and volunteers may need to have access to or use settings systems and/or data, such as governors, visiting IT staff or external speakers. It is important that, if you are responsible for or have invited a visitor, clear expectations are put in place regarding appropriate access and behaviour prior to access being permitted.

Password Policy

Staff must assume personal responsibility for usernames and passwords. Never use anyone else's username or password.

You must always keep your individual user name and password confidential. These usernames and passwords should never be disclosed to anyone. Passwords and user names should never be shared.

In some instances, users may be given the right to change passwords from the one originally issued.

Software

Software should be purchased or acquired from reputable vendors, in all cases following approval in writing from the Network Manager. Installation of any software (where staff have rights to do so) must be approved in writing by the Network Manager; no software may be installed by staff alone. Breach of this condition represents a large security and data protection risk, and may be grounds for disciplinary action.

Appendix 1

Student Acceptable Use Policy

This agreement forms part of the admissions pack all student receive when starting at Longhill High School.

LONGHILL HIGH SCHOOL
Student ICT Acceptable Use Policy (AUP)

All students must follow the conditions described in this and any other Acceptable Use policy of Longhill High School when using both school and personal ICT devices and accounts. Students will be provided with guidance by staff in the appropriate use of these electronic resources, but any use of a Longhill High School account remains the responsibility of the particular user. Check the website for more information.

Conditions of Use

Student access to the networked resources is a privilege, not a right. Students will be expected to use the resources for the educational purposes. It is the personal responsibility of every student to take all reasonable steps to make sure they follow the conditions set out in this and any other Acceptable Use Policy.

Acceptable Use

Students are expected to use the school network systems and personal devices, such as mobile phones in a responsible manner. The following list must be followed:

- I will only access websites that are appropriate and have been agreed by my teacher.
- I will use appropriate language when using ICT and will act in accordance with the schools' expectations and the advice given in this policy. Illegal activities of any kind are strictly forbidden.
- I will not use electronic devices to record any student or adult activities (e.g. sound, photos, and videos) without explicit written consent.
- I will not upload to the internet any text, sounds, photos or videos that aims to cause distress to students, teachers or the wider school community.
- I will not use language that could stir up hatred against any ethnic, religious or other minority group or generally undermines the dignity and respect of any individual or group.
- I will not reveal any personal information (e.g. home address, telephone number) about myself or other users over the network.
- I will not share my login details (including passwords) with anyone else. Likewise, I will never use other people's username and password.
- I will not attempt to visit websites that might be considered inappropriate or illegal. I am aware that downloading some material is illegal and the police or other authorities may be called to investigate such use.

- I will not attempt to change, damage or destroy any equipment, work of another user on the school network, or even another website or network connected to the school system.
- I agree to comply with the acceptable use policy of any other networks that I access.

UNACCEPTABLE USE
Examples of unacceptable use include, but are not limited to:

- Violating the privacy or dignity of other users, including staff, students and other members of the community
- Creating, transmitting, displaying or publishing any material (text, images or sounds) likely to harass, cause offence, inconvenience, anxiety or distress to any other person
- Bringing the school into disrepute and / or causing distress to staff, students or members of the wider community
- Searching for and downloading illegal material

SANCTIONS:

If students fail to comply with this policy they may have their internet, email and/or computer use restricted for a period of time or withdrawn altogether. Student personal devices, such as mobile phones, maybe confiscated for a period of time or the privilege to bring it into school removed.

Breaking the Student Acceptable Use Policy may lead to:

- Withdrawal of the student's access.
- Close monitoring of the students network activity.
- Investigation of the students past network activity.
- Disciplinary action, including a recommendation for temporary or permanent exclusion.
- In some cases, criminal prosecution.

Use of Social Media / Cyber Bullying
The school takes the issue of Cyberbullying and the appropriate use of Social Media very seriously. Students should not be accessing social media sites unless they have reached the minimum age requirement; such as

- Facebook 13 Years
- Instagram 13 Years
- Twitter 13 Years

If parents allow children to use these and other similar social media sites before they are old enough the school will not take responsibility for resolving issues that may occur.

THE USE OF ICT AND THE LAW

The use of ICT will always leave evidence no matter where the incident occurred; home computer, school computer, and/or mobile phone. The user will leave a 'digital footprint' that can potentially be used to identify them.

Misusing ICT can be a criminal offence under a range of different laws including:

- The Protection from Harassment Act 1997
- The Malicious Communications Act 1988
- Section 127 of the Communications Act 2003
- Public Order Act 1986

- The Defamation Acts of 1952 and 1996
- Computer Misuse Act 1990
- Crime and Disorder Act 1998
- Police and Justice Act 2006

For more advice on using ICT safely please visit the following website www.thinkuknow.co.uk

By ticking the relevant box on the parent/student consent form, I agree to the above policy.

Appendix 2

Social Networking Policy for Longhill High School

1. Introduction

1.1. The internet provides a range of social media tools that allow users to interact with one another, for example from rediscovering friends on social networking sites such as Facebook to keeping up with other people's lives on Twitter and maintaining pages on internet encyclopaedias such as Wikipedia.

1.2. Whilst the widespread availability and use of social networking applications brings opportunities to engage and communicate with audiences in new and exciting ways, it is important to ensure that we balance this not only with our legal responsibilities to safeguard and protect our children and staff but also with the need to safeguard the school image and reputation.

1.3. The school E Safety Policy which includes a wider range of information on home and school ICT use, security & safeguarding issues (including how all school staff will be made aware of relevant issues and whom they should contact within the school if any concerns arise) should be read alongside this policy, as well as all relevant school policies concerning data and technology in all aspects.

2. Purpose

2.1 The purpose of this policy is to:

- support safer working practice by setting out the key principles and expected standards of behaviour when using social networking media
- ensure all children are safeguarded
- ensure the reputation of the school (its staff, pupils and governors at the school) are not damaged or compromised
- ensure that any users are able to clearly distinguish where information provided via social networking applications is legitimately representative of the School
- minimise the risk of misplaced or malicious allegations being made against those who work with pupils
- reduce the incidence of positions of trust being abused or misused
- ensure the school, its governors and staff are not exposed to legal risks

3. Scope

3.1 This policy applies to the governing body, all teaching and other staff, whether employed by Brighton & Hove City Council or employed directly by the school, individual governors, external contractors providing services on behalf of the school or the City Council, teacher trainees and other trainees, supply staff, agency workers, volunteers and other individuals who work for, or provide services on behalf of, the school. These individuals are collectively referred to as 'staff members' in this policy.

3.2 This policy cannot cover all eventualities and, therefore, staff members should consult the Headteacher, ICT Manager and/or Data Protection Officer if they are in any way unsure about what is and isn't acceptable use of social media.

4. Legal Framework

4.1 Longhill High School is committed to ensuring that all staff members provide confidential services that meet the highest standards. All individuals working on behalf of the school are bound by a legal duty of confidence and other laws to protect the confidential information they have access to during the course of their work. Disclosure of confidential information on social media is likely to be a breach of the law and professional codes of conduct.

4.2 Confidential information includes, but is not limited to:

- Person-identifiable information, e.g. pupil and employee records protected by the Data Protection Act 1998
- Information divulged in the expectation of confidentiality
- School or Brighton & Hove City Council business or corporate records containing organisationally or publicly sensitive information
- Any commercially sensitive information such as information relating to commercial proposals or current negotiations
- Politically sensitive information

4.3 Staff members should also be aware that other laws relating to libel, defamation, harassment and copyright may apply to information posted on social media.

4.4 Longhill High School and Brighton & Hove City Council could be held vicariously responsible for acts of their employees in the course of their employment. For example, staff members who harass co-workers online or who engage in cyberbullying or discrimination on the grounds of race, sex, disability, etc. or who defame a third party while at work may render the school or the County Council liable to the injured party.

5. Definition of Social Media

5.1 Social media is the term commonly used for websites which allow people to interact with each other in some way by sharing information, opinions, knowledge and interests. Social networking websites such as Facebook, Bebo and MySpace are perhaps the most well-known examples of social media but the term also covers other web based services such as blogs, mircoblogs such as Twitter, chatrooms, fora, video and audio podcasts, open access online encyclopaedias such as Wikipedia, message boards, photo document, social bookmarking sites such as del.icio.us and content sharing sites such as flickr and YouTube.

5.2 This definition of social media is not exhaustive. The internet is a fast moving technology and it is impossible to cover all circumstances or emerging media. However, the principles set out in this policy must be followed irrespective of the medium.

5.3 For the purpose of this policy, the term social media also applies to the use of communication technologies such as mobile phones, cameras, PDAs / PSPs or other handheld devices and any other emerging forms of communications technologies.

6. Principles - Social Media Practice

6.1 Staff members need to be aware (and should assume) that everything they post online is public, even with the strictest privacy settings. Once something is online, it can be copied and redistributed and it is easy to lose control of it. They should therefore assume that everything they post online will be permanent and will be shared.

6.2 Staff members must be conscious at all times of the need to keep their personal and professional lives separate and to always maintain appropriate professional boundaries.

6.3 Staff members are responsible for their own actions and conduct and should avoid behaviour which might be misinterpreted by others or which could put them in a position where there is a conflict between their work for the school or Brighton & Hove City Council and their personal interests.

6.4 They must use social media in a professional, responsible and respectful way and must comply with the law, including equalities legislation, in their on-line communications.

6.5 Staff members must not engage in activities involving social media which might bring the school or the Council into disrepute.

6.6 They must not represent their personal views as those of the school or the Council on any social medium.

6.7 They must not discuss personal information about pupils, their family members, school or Council staff or any other professionals or organisations they interact with as part of their job on social media.

6.8 They must not name or otherwise identify pupils, former pupils or their parents, family members, colleagues etc. in social media conversations.

6.9 They must not use social media or the internet in any way to attack, insult, abuse, defame or otherwise make negative, offensive or discriminatory comments about pupils, their family members, colleagues, other professionals, other organisations, the school or the Council.

6.10 They must not browse, download, upload or distribute any material that could be considered inappropriate, offensive, defamatory, illegal or discriminatory.

6.11 They must at all times act in the best interests of children and young people when creating, participating in or contributing content to social media sites.

7. Personal Use of Social Media

7.1 Staff members need to be aware of the dangers of putting personal information such as addresses, home and mobile phone numbers, email addresses etc. onto social networking sites.

7.2 Staff members should ensure that they set the privacy levels of their personal sites at the maximum and opt out of public listings on social networking sites to protect their privacy.

7.3 Staff members should keep any passwords confidential, change them often and be careful about what is posted online. It is a good idea to use a separate email address just for social networking so that any other contact details are not disclosed.

7.4 Staff members should not identify themselves as employees of the school or Brighton & Hove City Council or service providers for the school or the City Council in their personal webspace. This is to prevent information on these sites being linked with the school or the Council. Where possible it may be useful to add a disclaimer such as “these are my own views and opinions and not those of my employer”

7.5 Taking the steps outlined in paragraphs 7.2 to 7.4 will avoid the potential for staff members to be contacted by pupils or their families or friends outside of the school environment and will reduce the chances of them becoming victims of identity theft.

7.6 All staff members should try to regularly review their social networking sites to ensure that information available publicly about them is accurate and appropriate. This should be suggested to new staff when they join the school. It is also good practice to close old accounts as they may contain personal information about you.

7.7 Staff members must not give their personal contact details including details of any blogs or personal social media sites or other websites to pupils or former pupils. It is also important to be aware that ex pupils may still have siblings in the school. Please refer to your schools own e-safety policy for more specific information. Please also see point 2.1 of this policy.

7.8 Staff members must not have contact through any personal social medium with any pupil, whether from this or any other school, unless the pupil is a family member or it is through school approved sites as part of official collaborative work. See point 7.11 below.

7.9 The school does not expect staff members to discontinue contact with their family members via personal social media once the school starts providing services for them. However, any information staff members obtain in the course of their employment must not be used for personal gain nor be passed on to others who may use it in such a way.

7.10 It is strongly recommended that staff members do not have any contact with pupils' family members through personal social media. Please see point 6.1 & 6.2 above.

7.11 If staff members wish to communicate with pupils through social media sites or to enable pupils to keep in touch with one another, they can only do so with the approval of the school and through official school sites.

7.12 Staff members must not establish, or seek to establish, social contact via social media/other communication technologies with pupils or ex-pupils and must never 'friend' a pupil or ex-pupil through social media. These actions could be construed as being part of a 'grooming process' in the context of sexual offending. This should be echoed in the school's policy also. In the case of some social networking sites it is possible to be 'followed' by a pupil without your consent. If this is the case, then your school should be informed and the pupil 'follower' deleted.

7.13 Staff members must never use or access pupils' social networking sites.

7.14 Staff members must decline 'friend requests' from pupils they receive in their personal social media accounts. If they receive such requests from pupils who are not family members, they must discuss these in general terms in class and signpost pupils to become 'friends' of the official school site or follow the school's own policy.

7.15 Confidentiality needs to be considered at all times. Social networking sites have the potential to discuss or publish inappropriate information. Staff members must therefore make sure that they do not publish confidential information that they have access to as part of their employment on their personal webspace. This includes personal information about pupils, their family members, colleagues, Brighton & Hove City Council staff and other parties as well as school or City Council related information. This requirement continues after they have left employment.

7.16 Similarly, photographs, videos or any other types of image of pupils and their families or images depicting staff members wearing school or City Council uniforms or clothing with school or City Council logos or images identifying sensitive school or Council premises (e.g. care homes, secure units) must not be published on personal webspace.

7.17 The school or Council corporate, service or team logos or brands must also not be used or published on personal webspace.

7.18 Staff members must not use school or City Council email addresses and other official contact details for setting up personal social media accounts or for communicating through such media.

7.19 Staff members must not edit open access online encyclopaedias such as Wikipedia in a personal capacity at work. This is because the source of the correction will be recorded as the employer's IP address and the intervention will, therefore, appear as if it comes from the employer itself.

1.20 Staff members are advised to be cautious about inviting work colleagues to be 'friends' in personal social networking sites. Social networking sites blur the line between work and personal lives and this may make it difficult to maintain professional relationships or embarrassing if too much personal information is known in the work place.

1.21 On leaving the service of Longhill High School, staff members must not contact Longhill High School pupils by means of personal social media sites. Similarly, staff members must not contact pupils from their former schools by means of personal social media.

2. Breaches of the Policy

8.1 Any breach of this policy may lead to disciplinary action, including the possibility of dismissal being taken against the staff member/s involved in line with Longhill High School or Brighton & Hove City Council Disciplinary Procedure/s.

8.2 Contracted providers of Longhill High School or Brighton & Hove City Council services must inform the Headteacher immediately of any breaches of this policy so that appropriate action can be taken to protect confidential information and limit the damage to the reputation of the school and the Council. Any action against breaches should be according to contractors' internal disciplinary procedures.