Church Hill Infant School

Authorised Acceptable Use Policy

(Staff, Governors and Volunteers)

This policy was reviewed January 2016

Signed_____

Dated_____

Why have an Authorised Acceptable Use Policy?

An Authorised Acceptable Use Policy is about ensuring that you, as a member of staff/volunteer/School Governor at Church Hill Infant School can use the Internet, email and other technologies available at the school in a safe and secure way. The policy also extends to out of school facilities e.g. equipment; printers and consumables; Internet and email, managed learning environment and websites.

An Authorised Acceptable Use Policy also seeks to ensure that you are not knowingly subject to **identity theft** and therefore **fraud**. Also that you **avoid cyber-bullying** and just as importantly, you **do not become a victim of abuse**. We have also banned certain sites which put the school network at risk.
Help us, to help you, keep safe.

Church Hill Infant School strongly believes in the educational value of ICT and recognises its potential to enable staff in delivering and supporting the curriculum. Church Hill Infant School also believes that it has a responsibility to educate its pupils; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the Internet and other related technologies. To this end the expectation of Church Hill Infant School is that both staff and volunteers will play an active role in implementing school and departmental Internet safety polices through effective classroom practice.

Church Hill Infant School recognises that for staff and volunteers to effectively deliver and support the curriculum they must be able to make use of the ICT facilities of the School and have the opportunity to expand and develop the teaching material associated with their work. However, Church Hill Infant School expects that both staff and volunteers, will at all times, maintain an appropriate level of professional conduct in their own use of the School's ICT facilities.

Listed below are the terms of this agreement. Staff, School Governors and volunteers are expected to use the ICT facilities of the School in accordance with these terms. Violation of these terms is likely to result in disciplinary action in accordance with Leicestershire County Council Disciplinary Procedures for Local Government Services Employees. Where the policy is breached in by either volunteers or governors the School will seek to advice and support from the Local Authority in order to manage the situation in a fashion that safeguards the school population.

Please read this document carefully and sign and date it to indicate your acceptance of the terms herein.

1. Equipment

1.1 School Computers

All computers and associated equipment are the property of Church Hill Infant School and must be used in accordance with this policy which adheres to the Computer Misuse Act 1990 and the Data Protection Act 1998 (see Glossary). The Head Teacher and the ICT coordinator in liaison with Technical Support Service assume responsibility of maintenance of all hardware and software. Mis-use of equipment includes, but is not limited to the following:

- Modification or removal of software
- Unauthorised configuration changes
- Creation or uploading or computer viruses or other malware
- Deliberate deletion of files.
- The uploading of computer files to the School's network

Any of these actions reduces the availability and reliability of computer equipment, puts other users' data at risk and increases downtime caused by repairs, thus delaying other essential work such as upgrades or enhancements.

1.2 Laptop Computers

Laptop computers are issued to all teaching staff as required. Laptops remain the property of Church Hill Infant School all times, and their usage is subject to the following guidelines:

- The equipment remains the property of Church Hill Infant School at all times and must be returned to the School at the end of the lease agreement or contractual period.
- Maintenance of the equipment is the responsibility of Church Hill Infant School. All maintenance issues must be referred to the ICT coordinator and logged, through the usual channels.
- All installed software MUST be covered by a valid license agreement held by Church Hill Infant School.
- All software installation MUST be carried out by the school's Technical Support Service in accordance with the relevant license agreements.
- No software should be removed, uninstalled or disabled under any circumstances. Any software problems should be reported through the usual support channels.
- Antivirus software must be updated regularly.
- The user of the equipment is responsible for all personal files and data stored on the equipment. Backup of the data is the responsibility of the user. It is strongly recommended that all data is regularly backed up, either to a CDRW disk, an encrypted memory stick or to the Church Hill Infant School network. Where removable media is used the user must ensure that these mediums have not been used to download materials that are at risk of damaging the network. It is recommended that the school's facility to transfer files is used.
- The user of the equipment must not encrypt <u>any</u> data or password protect any files so as to ensure future usage of the equipment.
- Church Hill Infant School cannot be held responsible for loss of data in the event of either a hardware or software failure or user error.

- From time to time, it may be necessary for the school's Technical Support Service to perform software updates and maintenance for which the equipment must be made available in School when reasonably requested.

1.3 Use of Removable Storage Media

Whilst staff may use CD disks or encrypted flash memory devices to transfer files between home and school, Church Hill Infant School cannot guarantee the correct operation of any removable media or the integrity of any data stored on it.

1.4 Printers and Consumables

Printers are provided across the School for educational or work-related use only. All printer usage can be monitored and recorded.

- Always print on a black & white printer unless colour is absolutely essential
- Proof-read your document on-screen and use the 'Print-Preview' facility to check the layout before printing.
- Do not print unnecessarily or waste ink or paper.
- Avoid printing directly from the Internet where possible. Internet pages are often not suitably formatted for printing and may cause wastage of paper and other consumables.
- Use the secure print option when printing stickers in order to avoid any wastage and limit confidential papers being viewed by others.

1.5 Data Security and Retention

All data stored on the Church Hill Infant School network is backed up daily and backups are stored for at least two months. If you should accidentally delete a files or files in your folder or shared area, please inform the SBM immediately so that it can be recovered. Generally, it is not possible to recover files that were deleted more than 2 months previously.

2. Internet and Email

2.1 Content Filtering

Church Hill Infant School provides Internet filtering, designed to remove controversial, offensive or illegal content. However, it is impossible to guarantee that all controversial material is filtered. If you discover any websites containing inappropriate or offensive content, please report these to the Headteacher so that they can be filtered. If you wish for a website to be unfiltered then pleased contact the Technican using the appropriate methods. All websites visited for school / educational purposes only.

2.2 Acceptable use of the Internet

Use of the Internet should be in accordance with the following guidelines:

- Transmission of any material in violation of any United Kingdom or other national laws is prohibited. This includes, but is not limited to, copyrighted material, threatening or obscene material or material protected by trade laws

- Only access suitable material – Using the Internet to obtain, download, send, print, display or otherwise transmit or gain access to materials which are unlawful, obscene or abusive is not permitted.

- Respect the work and ownership rights of people outside the School. This includes abiding by copyright laws.

- Do not access Internet chat sites. These represent a significant security threat to the School's network.

- The use of online gaming sites is prohibited. These consume valuable network resources that may adversely affect the performance of the system.

- Do not attempt to download or install software from the Internet. The ICT Coordinator in liaison with technical support service assumes responsibility for all software upgrades and installations.

- Staff are reminded that ALL Internet access is logged and actively monitored and traceable.

2.3 Email

Staff are provided with an email address by Church Hill Infant School. This may be used for any legitimate educational or work-related activity. Staff should use the email in accordance with the following guidelines and are reminded that the School retains the right to monitor email communications at any time if this is deemed necessary.

The sending or receiving of messages which contain any inappropriate material is strictly forbidden. This material includes, but it not limited to, pornography, unethical or illegal requests, racism, sexism, inappropriate language, or any other use which may be likely to cause offence. Disciplinary action will be taken in all cases.

- Messages relating to, or in support of any illegal activities may be reported to the authorities.

- Do not download or open file attachments unless you are certain of both their content and origin. File attachments may contain viruses or other forms of malware that may cause loss of data or damage to the School network.

- Staff should not send personally identifiable information by email, as it is not a secure medium.

3. External Services

Church Hill Infant School provides a number of services that are accessible externally, using any computer with an Internet connection. These should be used strictly for educational or work-related activities only and in accordance with the following guidelines.

Remote access to the server is available to teaching staff and senior management only. The IP addrees should be kept secure at all times.

4.0 Privacy and Data Protection

4.1 Passwords

- Never reveal your password to anyone else or ask others for their password.

- When choosing a password, choose a word or phrase that you can easily remember, but not something which can be used to identify you or be easily guessed (Use capital letters, numbers and symbols).

- If you forget your password, please request that it be reset via ICT Coordinator

4.2 Security

- Never attempt to access files or programs to which you have not been granted authorisation. Attempting to bypass security barriers may breach data protection regulations and such attempts will be considered as hack attacks and will be subject to disciplinary action.

- You should report any security concerns immediately Church Hill Infant School

- Any user identified as a security risk will be denied access to the system and subject to disciplinary action in accordance with Leicestershire County Council Disciplinary Procedures for Local Government Services Employees.

5.0 Management and Information Systems

Access to MIS software is available only from designated locations and only to those staff who require it. Access is subject to agreement with the Headteacher. Usage of MIS software is subject to the following guidelines:

- Password security is vital. If you believe that your password has been discovered by a student or other member of staff, **change it immediately**.

- If you leave your computer unattended, particularly in a classroom, either log out or lock it by using the CTRL-ALT-Delete keys and then choosing "Lock Workstation". Once this is done, you will need to re-enter your password to gain access to the computer.

- Joining administration and curriculum networks raises issues regarding who within the school organisation has access to data. Within Church Hill Infant School it is understood that the Headteacher and Senior Leadership team have a clear duty of care to protect the access to confidential data. Further details regarding this aspect of the School's E-safety approach can be found in Appendix G (Management and Information Systems).

6.0 Mobile Technologies

For reasons of safety and security staff, governors and volunteers should not use their mobile phone or any other technology in a manner that is likely to bring the school into disrepute or risk the welfare of a child or young person.

The development of mobile technology is such that mobile phones and other similar devices connected to mobile networks have enhanced features which include: picture messaging; mobile access to the Internet; entertainment in the form of video streaming and downloadable video clips from films, sporting events, music and games etc. The capabilities of 3G mobile phones also means that adults working within the school environment may be sent inappropriate images or videos, or be encouraged to send back images or video of themselves using integrated cameras.

Personal mobiles

This guidance is in place to avoid the use of mobile phones causing unnecessary disruptions and distractions within the workplace, and to ensure effective safeguarding practice and to protect against potential misuse.

In the interests of equality, and to further promote safety, the guidance applies to any individual who has a mobile phone on site, including children, parents and visitors, as detailed below:

• Staff are permitted to have their mobile phones about their person; however there is a clear expectation that all personal use is limited to allocated lunch and/or tea breaks.
• Other than in agreed exceptional circumstances, phones must be switched off and calls and texts must not be taken or made during lesson time or any time when supervising children or talking with parents.
• Staff are not permitted, in any circumstance to use their phones for taking, recording or sharing images.
• Staff, visitors and contractors are respectfully requested not to use their mobile phones in school. Should phone calls and/or texts need to be taken or made this should be done outside the school building to avoid unnecessary disturbance or disruption to others.

If you are sent inappropriate material e.g. images or videos **report it immediately**.
not permitted to use their own personal phones for contacting children, young people and their families within or outside of the setting.

7.0 Support Services

All ICT hardware and software maintenance and support requests should be submitted to the ICT Coordinator using one of the following methods

- Logged in ICT maintenance report book which is kept in the school staff room

The ICT coordinator will monitor the requests made and will make every effort to ensure that all technical or operational problems are resolved within a reasonable time.

7.1 Software Installation

The Headteacher and ICT coordinator in liaison with technical support service will assume responsibility for all software installation and upgrades. Staff may request the installation of new software packages onto the network, but this will be subject to the following:

- A minimum of 3 weeks is required for the installation of new software.
- Software cannot be installed on the School's network without a valid license agreement. This must be supplied with the software package.
- Please check the licensing terms of the software package carefully to ensure that it is suitable for use on the School network. If you are unsure, please ask the ICT coordinator for assistance or contact the software supplier. A relevant and valid license agreement document will be required before any software packages can be installed.
- All software installation media and license agreements are held centrally within the School to aid in license tracking and auditing. Installation media cannot normally be released except by special agreement.
- When purchasing new software for use on the School network, please check its suitability, compatibility and licensing terms with the Headteacher and ICT coordinator. Purchase orders for new software will normally be authorised only with the agreement of the Headteacher.

7.2 Service Availability

Whilst every effort is made to ensure that the systems, both hardware and software are working correctly, the School will not be responsible for any damages or loss incurred as a

result of system faults, malfunctions or routine maintenance. These damages include loss of data as a result of delay, non-deliveries, mis-deliveries or service interruptions caused by the system or elements of the system, or your errors or omissions. Use of any information obtained via the School ICT system is at your own risk. Church Hill Infant School specifically denies any responsibility for the accuracy of information obtained whilst using the ICT systems.

Glossary

- Computer Misuse Act

  The Computer Misuse Act makes it an offence for anyone to have:-

  - Unauthorised access to computer material e.g. if you find or guess another user's password and use it.
  - Unauthorised access to deliberately commit an unlawful act e.g. if you guess another user's password and access their learning account without permission
  - Unauthorised changes to computer material e.g. if you change the desk-top set up on your computer or introduce a virus deliberately to the school's network system.

- Data Protection Act 1998

  The Data Protection Act ensures that information held about you is used for specific purposes only. These rules apply to everyone in the school.

  The Act covers the collection, storing, editing, retrieving, disclosure, archiving and destruction of data held about individuals in the school. The Act not only applies to paper files it also applies to electronic files.

  The Principles of the Act state that data must be:

  - Fairly and lawfully processed
  - Processed for limited purposes
  - Adequate, relevant and not excessive
  - Accurate and up to date
  - Kept no longer than necessary
  - Processed in accordance with data subject's rights
  - Secure
  - Not transferred to other countries without adequate protection

- RIPA – Regulation of Investigatory Powers Act 2002
  If a request for authorised access is made to the school they will provide the appropriate access to your ICT records and files. The Act legislates for using methods of surveillance and information gathering to help the prevention of crime, including terrorism. RIPA makes provision for:
  - the interception of communications
  - the acquisition and disclosure of data relating to communications
  - the carrying out of surveillance
  - the use of covert human intelligence sources
  - access to electronic data protected by encryption or passwords

  If a request for authorised access is made to the school, we will provide the appropriate access to your ICT records and files.

Policy Reviewed: Jan 2016

REQUIRED SIGNATURE

MEMBER OF STAFF/VOLUNTEER

I understand and agree to the provisions and conditions of this agreement. I understand that any violations of the above provision may result in disciplinary action and revocation of privileges. I also agree to report any misuse of the system to the Headteacher. I agree to use the Internet and electronic communications systems in compliance with the terms outlined in this document and understand that my Internet access and any electronic communications may be logged or monitored.

NAME

_____

SIGNATURE

_____

DATE

_____