Authorised Acceptable ICT Use Policy (Staff, Governors and Volunteers) – The Pochin School

Introduction
- This policy was revised during the Autumn Term of 2013 through a process of consultation with the teachers and teaching assistants and approved by the Governing Body on 21 January 2014. It will be reviewed in accordance with the School Development Plan.

**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 The Pochin 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.

The Pochin School strongly believes in the educational value of ICT and recognises its potential to enable staff in delivering and supporting the curriculum. The Pochin 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 The Pochin School is that both staff and volunteers will play an active role in implementing the school's Internet safety polices through effective classroom practice.

The Pochin 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, The Pochin 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 The Pochin 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 Pochin School assumes 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 and support staff as required. Laptops remain the property of The Pochin School at all times, and their usage is subject to the following guidelines:

- The equipment remains the property of The Pochin 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 The Pochin School. All maintenance issues must be referred to the Headteacher, through the usual channels.
- All installed software MUST be covered by a valid license agreement held by The Pochin School.
- All software installation MUST be carried out by the Headteacher 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. For laptop computers, it will be necessary to connect them to the School network to update the antivirus software. *This should be done at least weekly*.
- 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, a memory stick or to The Pochin 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.
- The Pochin 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 Headteacher 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 flash memory devices to transfer files between home and school, The Pochin School cannot guarantee the correct operation of any removable media or the integrity of any data stored on it. It should be noted that rewriteable CDs in particular are neither robust nor reliable, and should not be used as the sole means of storage for important files. The Pochin School cannot guarantee the correct operation of flash memory devices on the system, although every effort is made to ensure that this facility is available.

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.

2. Internet and Email

2.1 Content Filtering

The Pochin 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.

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 print out pages directly from a website. Web pages are often not suitably formatted for printing and this may cause significant wastage of paper. If you wish to use content from websites, consider using the copy and paste facility to move it into another application, copyright permitting.
- Do not attempt to download or install software from the Internet. The headteacher 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 The Pochin 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.
- Whilst it is possible to attach files to an email message, staff are advised that that email is not generally suited to transferring large files. Whilst there are no hard and fast rules regarding file sizes that can be attached to an email message, files exceeding approximately 5MByte in size are generally considered to be excessively large and staff should consider using other methods to transfer such files.
- 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.

3.0 Privacy and Data Protection
3.1 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, such as your name or address. Generally, longer passwords are better than short passwords. It is advisable to use a 'strong' password. A strong password is one which contains a combination of upper and lower-case letters, numbers and other punctuation characters. You can substitute numbers and letters for other characters that look similar, such as '3' for 'E', '1' for 'I' or '@' for 'O', '!' for '1' etc. This will help to make your password much more difficult to guess. Remember that passwords are case-sensitive.
- If you forget your password, please request that it be reset via the headteacher.
- If you believe that a student or other staff may have discovered your password, then change it *immediately*.

3.2 Security
- o 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.
- o You should report any security concerns immediately to the headteacher.
- o 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.

4.0 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.

In order to reduce the opportunity for those behaviours that could possibly cause upset, it is advisable that staff, governors and volunteers working with children and young people within the school setting, limit their use of mobile technologies to necessary communication during specified breaks during the school day.

If you are sent inappropriate material e.g. images or videos **report it immediately**.

5.0 Support Services

All ICT hardware and software maintenance and support requests should be submitted to the headteacher.

6.0 ICT and Social Networking/Contact

Adults should not establish or seek to establish social contact with pupils for the purpose of securing friendship or to strengthen a relationship. If a pupil or parent seeks to establish social contact, or if this occurs coincidentally, the member of staff should exercise her/his professional judgment in making a response. There will be occasions when there are social contacts between pupils and staff, where for example the parent and teacher are part of the same social circle. These contacts however, will be easily recognised and openly acknowledged. Contact through social networking sites on the internet should not occur under any circumstances.

There must be awareness on the part of those working with children and young people that some social contacts, especially where these are not common knowledge, can be misconstrued as being part of a grooming process. This can also apply to social contact made through outside interests, through the staff members' own family or through social networking sites on the internet.

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.