Ullesthorpe C of E Primary School
Acceptable Use Policy M12

Signed by the Governing Body:
Agreed by the Governing Body: May 2016
Review Date: Summer 2019 or earlier if required.

Why have an Authorised Acceptable Use Policy?
An Authorised Acceptable Use Policy is about ensuring that you, as a member of staff/volunteer/governor at Ullesthorpe 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 environments 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.
Ullesthorpe strongly believes in the educational value of computing and recognises its potential to enable staff and volunteers in delivering and supporting the curriculum. Ullesthorpe 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 Ullesthorpe is that both staff and volunteers will play an active role in implementing school Internet safety polices through effective classroom practice.

Ullesthorpe recognises that for staff and volunteers to effectively deliver and support the curriculum they must be able to make use of the computing facilities of the School and have the opportunity to expand and develop the teaching material associated with their work. However, Ullesthorpe 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 computing facilities.

Listed below are the terms of this agreement. Staff, governors and volunteers are expected to use the computing facilities of the School in accordance with these terms. **Violation of these terms is likely to result in disciplinary action in accordance with School’s policy.** Where the policy is breached by either volunteers or governors the School will seek advice and support from HR in order to manage the situation in a fashion that safeguards the school population.

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

1. Equipment

1.1 School Computers

All computers and associated equipment are the property of Ullesthorpe 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 School and [any other company or named individual e.g. Network Manager] assumes responsibility of maintenance of all hardware and software. Misuse 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.

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 issued to teaching staff remain the property of Ullesthorpe all times, and their usage is subject to the following guidelines:

- The equipment remains the property of Ullesthorpe 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 Ullesthorpe. All maintenance issues must be referred to the Office Manager.
- All installed software MUST be covered by a valid license agreement.
- All software installation MUST be carried out 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 Internet 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 the Ullesthorpe 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 any data or password protect any files without the knowledge and approval of the Headteacher, so as to ensure future usage of the equipment.
- Ullesthorpe 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 ICT technician 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, Ullesthorpe 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. Ullesthorpe cannot guarantee the correct operation of flash memory devices on the system, although every effort is made to ensure that this facility is available. If a memory stick is used it must be encrypted in order to protect confidential data.

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 in black & white unless colour is 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 toner 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.

1.5 Data Security and Retention

All data stored on the Ullesthorpe network is backed up regularly onto an external hard-drive. If you should accidentally delete a files or files in your folder or shared area, please inform the Office Manager immediately so that, where possible, it can be recovered.

2. Internet and Email

2.1 Content Filtering

Ullesthorpe 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 Office Manager 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 or social networking 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.
- 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 Ullesthorpe. 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 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 10MByte 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. External Services

Ullesthorpe 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

3.1 Web-Email

Web email provides remote access to your email account from home or anywhere with an Internet connection. Use of this service is subject to the following guidelines. Staff should use 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.

- Web-email is provided for use of Ullesthorpe staff only. Access by any other party is strictly prohibited.
- By using Web-Email, you signify that you are an employee of Ullesthorpe, and that you have been authorised to use the system by the relevant School authority.
- Observe security guidelines at all times. Never reveal your password to anyone.
- Remember to treat file attachments with caution. File attachments may contain viruses or other forms of malware that may cause loss of data or damage to the computer from which you are working. Do not download or open file attachments unless you are certain of both their content and origin. Ullesthorpe accepts no responsibility for damage caused to any external equipment or software as a result of using the web-email service.
- The rules that apply to Email are also to Web-Email.

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, 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.
- If you believe that a student or other staff may have discovered your password, then change it immediately.

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 to the Office Manager.
- Any user identified as a security risk will be denied access to the system and subject to disciplinary action in accordance with School’s policy.

5.0 Management and Information Systems

Access to MIS software is available only from designated locations and only to those staff who require it. 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. You can also use the windows-L keys to lock the machine as well.
- Joining administration and curriculum networks raises issues regarding who within the school organisation has access to data. Within Ullesthorpe it is understood that the Headteacher and Senior Leadership team have a clear duty of care to protect the access to confidential data.

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/4G 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.

7.0 Support Services

All computing hardware and software maintenance and support requests should be submitted to the Office Manager who will make every effort to ensure that all technical or operational problems are resolved within a reasonable time.

7.1 Software Installation

The ICT technician assumes 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 two weeks’ notice is required for 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 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 Office Manager. 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, misdirected 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's computer infrastructure is at your own risk. Ullesthorpe specifically denies any responsibility for the accuracy of information obtained whilst using the computer infrastructure.

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.

Acceptable Use Agreement: All Staff, Volunteers and Governors

Covers use of all digital technologies in school: i.e. email, Internet, network resources, software, communication tools, equipment and systems.

- I will only use the school’s digital technology resources and systems for Professional purposes or for uses deemed ‘reasonable’ by the Head and Governing Body.
- I will not reveal my password(s) to anyone.
- I will follow ‘good practice’ advice in the creation and use of my password. If my password is compromised, I will ensure I change it. I will not use anyone else’s password if they reveal it to me and will advise them to change it.
- I will not allow unauthorised individuals to access email / Internet / network, or other school systems, or any Local Authority (LA) system I have access to.
- I will ensure all documents, data etc., are printed, saved, accessed and deleted / shredded in accordance with the school’s network and data security protocols.
- I will not engage in any online activity that may compromise my professional responsibilities.
- I will only use the approved email system(s) for any school business.

- I will only use the approved email system(s) with parents/carers, and only communicate with them on appropriate school business.
- I will not browse, download or send material that is considered offensive or of an extremist nature by the school.
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach or equipment failure to the appropriate line manager / school named contact.
- I will not download any software or resources from the Internet that can compromise the network or might allow me to bypass the filtering and security system or are not adequately licensed.
- I will check copyright and not publish or distribute any work including images, music and videos, that is protected by copyright without seeking the author’s permission.
- I will not connect any device (including USB flash drive), to the network that does not have up-to-date anti-virus software, and I will keep any ‘loaned’ equipment up-to-date, using the school’s recommended anti-virus and other ICT ‘defence’ systems.
- I will not use personal digital cameras or camera phones or digital devices for taking, editing and transferring images or videos of pupils or staff and will not store any such images or videos at home.
- I will follow the school’s policy on use of mobile phones / devices at school and will only use in staff areas.
- I will only use school approved equipment for any storage, editing or transfer of digital images / videos and ensure I only save photographs and videos of children and staff on the appropriate system or staff-only drive within school.
- I will ensure that any private social networking sites / blogs etc that I create or actively contribute to are not confused with my professional role.
- I will ensure, where used, I know how to use any social networking sites / tools securely, so as not to compromise my professional role.
- I agree and accept that any computer or laptop loaned to me by the school, is provided solely to support my professional responsibilities and that I will notify the school of any “significant personal use” as defined by HM Revenue & Customs.

- I will only access school resources remotely (such as from home) using the school approved system and follow e-security protocols to interact with them.
- I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow school data security protocols when using any such data at any location.
- I understand that data protection policy requires that any information seen by me with regard to staff or pupil information, held within the school's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.
- I will alert the designated child protection lead if I feel the behaviour of any child may be a cause for concern.
- I understand it is my duty to support a whole-school safeguarding approach and will report any behaviour of other staff or pupils, which I believe may be inappropriate or concerning in any way, to designated child protection lead.
- I understand that all Internet and network traffic / usage can be logged and this information can be made available to the Head / designated child protection lead on their request.
- I understand that Internet encrypted content (via the https protocol), may be scanned for security and/or safeguarding purposes.
- I will only use any LA system I have access to in accordance with their policies.
- Staff that have a teaching role only: I will embed the school's on-line safety / digital literacy / counter extremism curriculum into my teaching.

Acceptable Use Policy: Agreement Form: All Staff, Volunteers, Governors

User Signature

I agree to abide by all the points above.

I understand that I have a responsibility for my own and others e-safeguarding and I undertake to be a 'safe and responsible digital technologies user'.

I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school's most recent e-safety policies.

I understand that failure to comply with this agreement could lead to disciplinary action.

Signature .... Date..

Full Name .... (printed)

Job title / Role ....

Authorised Signature (Head Teacher / Deputy)

I approve this user to be set-up on the school systems relevant to their role

Signature .... Date ....

Full Name .... (printed)