LOVE God • LOVE Neighbour • LOVE Self

St Chad’s CofE Nursery and Infant School

# Staff ICT Acceptable Use Policy

|  |  |  |
|---|---|---|
| **School Leader:** | **K Gilsenan** |  |
| **Link Governor:** | **N Iqbal** |  |
| **Policy Approved** | **Signed: P Geary** | **Date: 06.06.18** |
| Policy Reviewed | Signed: M Scothbrook | Date: 17.11.21 |
| Policy Reviewed | Signed: N Iqbal | Date: 01.10.20 |
| Policy Reviewed | Signed: R Williams | Date: 19.06.19 |
| Policy Reviewed | Signed: | Date: |

**Statement of intent**
The Staff ICT Acceptable Use Policy has been designed to outline all responsibilities when using technology both on and off site, using personal and school devices and applies to all staff, volunteers, contractors and visitors.

This policy is divided into the following three sections:

- General policy and code of practice
- Internet policy and code of practice
- Email policy and code of practice

**Introduction**
As a professional organisation with responsibility for children's safeguarding it is important that all staff take all possible and necessary measures to protect data and information systems from malware, unauthorised access, damage, loss, abuse and theft. All members of staff have a responsibility to use the school's computer system in a professional, lawful, and ethical manner. To ensure that members of staff are fully aware of their professional responsibilities when using Information Communication Technology and the school systems, they are asked to read and sign this Acceptable Use Policy.

This is not an exhaustive list and all members of staff are reminded that ICT use should be consistent with the school ethos, other appropriate policies and the Law.

**General policy and code of practice**

- The school has well-developed and advanced ICT systems, which it intends for you to benefit from.
- This policy sets out the rules that you must comply with to ensure that the system works effectively for everyone.

**Privacy**

The GDPR and Data Protection Act 2018 require all personal and special category data to be processed with the utmost credibility, integrity and accuracy. This applies to all data the school stores on its network regarding staff, pupils and other natural persons it deals with whilst carrying out its functions.

The school will only process data in line with its lawful basis to uphold the rights of both pupils and staff and other third parties.

In order to protect pupils' safety and wellbeing, and to protect the school from any third party claims or legal action against it, the school may view any data, information or material on the school's ICT systems (whether contained in an email, on the network, notebooks or laptops) and in certain circumstances, disclose that data, information or material to third parties, such as the police or social services. The school's Privacy Policy details the lawful basis under which the school is lawfully allowed to do so.
The school disclaimer that automatically appears at the end of each of your emails notifies the recipient that any email correspondence between you may be monitored. You must not remove this disclaimer. You should bring to the attention of any person who wishes or intends to send you an email that the school may monitor the content of their email.

**Code of practice**

| | |
|---|---|
| The school's philosophy | In using ICT, you will follow the school's ethos and consider the work and feelings of others. You must not use the system in a way that might cause annoyance or loss of service to other users. |
| Times of access | The network is available during term time. Out of term time the network may be subject to maintenance downtime and so may not be available for brief periods. You will be notified of any changes. |
| User ID and password and logging on | You will be given your own user ID and password. You must keep these private and not tell or show anyone what they are.<br>Your password must be a mix of the following:<br>• Contain at least six characters<br>• A mixture of lower case and capital letters<br>• At least one numbers<br>• At least one symbol<br>If you forget or accidentally disclose your password to anyone else, you must report it immediately to a member of the ICT support staff.<br>You must not use another person's account or allow another person to use your account. The facilities are allocated to you on a personal basis and you are responsible for the use of the machine when you are logged on. The school's system records and senior ICT staff monitor your use of the system.<br>Use of the school's facilities by a third party using your user name or password will be attributable to you, and you will be held accountable for the misuse.<br>You must not log on to more than one computer at the same time. |
| Printing | The school may wish to check that expensive resources are being used efficiently and the member of staff may suggest other strategies to you to save on resources. |
| Logging off | You must log off from the computer you are using at the end of each of your sessions and wait for the standard login screen to reappear before leaving.<br>This signals to the system that you are no longer using the service; it ensures security and frees up resources for others to use. |
| Access to information not normally available | You must not use the system or the internet to find or use facilities or flaws in the system that might give access to information or areas of the network not normally available.<br>You must not attempt to install software to explore or harm the system. Use of hacking tools, e.g. 'loggers', 'sniffers' or 'evidence elimination software', is expressly forbidden. |
| Connections to the system | You must not connect any hardware which may be detrimental to the school's network. |

| | |
|---|---|
| Connections to the computer | You should use the keyboard, mouse and any headphones provided. You must not adjust or alter any settings or switches without first obtaining the written permission of a member of the ICT staff.<br>You must never attempt to use any of the connectors on the back of any desktop computer.<br>You may use the encrypted USB memory sticks, or other portable storage media where a port is provided on the front of the computers.<br>You are not permitted to connect anything else to the computer without first getting the permission of a member of the ICT staff. |
| Virus | If you suspect that your computer has a virus, you must report it to a member of the ICT staff immediately. |
| Installation of software, files or media | You must not install or attempt to install software of any kind to network drives or local hard drives of networked desktop computers.<br>You must not alter or re-configure software on any part of the school’s system. |
| File space | You must manage your own file space by deleting old data rigorously and by deleting emails that you no longer require.<br>If you believe that you have a real need for additional space, please discuss this with a senior member of the ICT support staff.<br>Read through files annually saved on the main server. Achieve or delete files that are no longer needed to save space. |
| Transferring files | You may transfer files to and from your network home directories using and encrypted USB/removable devices.<br>When transferring files to and from your network home directories, you must not import or export any material unless the owner of that material expressly permits you to do so. |
| Reporting faults and malfunctions | You must report any faults or malfunctions by email to Mercury Helpdesk (Autotask) helpdesk@mercuryavs-ltd.co.uk, including full details and all error messages, as soon as possible. |
| Food and drink | You must not eat or drink, or bring food or drink, including sweets and chewing gum, near school ICT equipment.<br>You must always maintain a clean and quiet working environment. |
| Copying and plagiarising | You must not plagiarise or copy any material which does not belong to you. |
| Copies of important work | It is your responsibility to keep all work saved on the main server. Work is backed up remotely and saved for a limited time. Please contact the ICT lead as soon as possible, if any work is missing or lost on the school system. |

| | |
|---|---|
| | Any data containing personal and special category data must not be stored on unencrypted media and paper back-ups must be stored in a secure lockable location. |
| Using school equipment off site | All equipment must be signed out before leaving the school premises:<br>IPads: sign out sheet on top of the IPad trolley. Please note the IPad number displayed on the back of the IPad<br>Long term use of school surfaces or laptops are logged by mercury<br>• Data is collected, processed, transported, and used in accordance with the school's DDAT Data Protection Policy.<br>• The staff members who are taking data from the school to fulfil their roles at home take full responsibility for the security of the data.<br>• Staff members are advised to ensure that they have their own domestic insurance policies in places for household contents and buildings.<br>• All electronic devices used in transferring data between the school and staff members' homes are password-protected to secure information in case of theft.<br>• Staff members are not permitted to let their family members or friends use any school equipment. |

**Online safety policy and code of practice**

The school can provide access to the internet from desktop PCs/surfaces/laptops via the computer network and through a variety of electronic devices connected wirelessly to the network.

Whenever accessing the internet using the schools or personal equipment you must observe the code of practice below.

This policy and code of practice is designed to reduce and control the risk of offences being committed, liabilities being incurred, staff or other pupils being offended and the school's facilities and information being damaged.

Any breach of this policy and the code of practice will be treated extremely seriously, and it may result in disciplinary or legal action or expulsion.

The school may take steps, including legal action where appropriate, to recover from an individual any expenses or liabilities the school incurs because of the breach of this policy and code of practice.

**Why is internet access available?**

The internet is a large and very useful source of information. Numerous websites and services, both official and unofficial, provide information or links to information which would be useful for educational purposes.

**Why is a code of practice necessary?**

There are four main issues:

- Although the internet is often described as 'free', there is a significant cost to the school for using it. This cost includes telephone line charges, subscription costs (which may depend on how much a service is used) and the computer hardware and software needed to support internet access.
- Although there is much useful information on the internet, there is a great deal more material which is misleading or irrelevant. Using the internet effectively requires training and self-discipline. Training is available on request from the ICT lead.
- Unfortunately, the internet carries a great deal of unsuitable and offensive material. It is important for legal reasons, reasons of principle, and to protect to protect the staff and pupils who access to the internet, that it is properly managed. Accessing certain websites and services, and viewing, copying or changing certain material, could amount to a criminal offence and give rise to legal liabilities.
- There is a danger of importing viruses on to the school’s network, or passing viruses to a third party, via material downloaded from or received via the internet, or brought into the school on disks or other storage media.

**Code of practice**

| | |
|---|---|
| Use of the internet | The Internet should not be used for private or leisure purposes. It is provided primarily for education or business use. |
| Inappropriate material | You must not use the internet to access any newsgroups, links, list-servers, web pages or other areas of cyberspace that could be offensive because of pornographic, indecent, racist, violent, illegal, illicit, or other inappropriate content. "Inappropriate" in this context includes material which is unsuitable for viewing by pupils.<br>You are responsible for rejecting any links to such material which may appear inadvertently during research.<br>If you encounter any material which could be regarded as offensive you must leave that website or service immediately and not make any copy of that material. If you encounter any difficulty in leaving a website or service, you must inform the ICT support staff immediately. |
| Misuse, abuse and access restrictions | You must not misuse or abuse any website or service or attempt to bypass any access controls or restrictions on any website or service. |
| Giving out information | You must not give any personal information concerning the school, children or parents, or any member of staff when accessing any website or service. This prohibition covers the giving of names of any of these people – the only exception being the use of the school’s name and your name when accessing a service which the school subscribes to. |
| Personal safety | You should take care with who you correspond with.<br>You should not disclose where you are or arrange meetings with strangers you have got in contact with over the internet. |

| | |
|---|---|
| Hardware and software | You must not make any changes to any of the school's hardware or software. This prohibition also covers changes to any of the browser settings.<br>The settings put in place by the school are an important part of the school security arrangements and making any changes, however innocuous they might seem, could allow hackers and computer viruses to access or damage the school's systems. |
| Copyright | You should assume that all material on the internet is protected by copyright and must be treated appropriately and in accordance with the owner's rights.<br>You must not copy, download or plagiarise material on the internet unless the owner of the website expressly permits you to do so. |

**Email policy and code of practice**

The school's computer system enables members of the school to communicate by email with any individual or organisation with email facilities throughout the world.

For the reason outlined above, it is essential that a written policy and code of practice exists, which sets out the rules and principles for use of email by all.

Any breach of this policy and code of practice will be treated seriously and it may result in disciplinary or legal action or expulsion.

The school may take steps, including legal action where appropriate, to recover from an individual any expenses or liabilities the school incurs because of the breach of this policy and code of practice.

**Code of practice**

| | |
|---|---|
| Purpose | You should only use the school's email system for work related emails.<br>You are only permitted to send a reasonable number of emails. |
| Trust's disclaimer | The school's email disclaimer is automatically attached to all outgoing emails and you must not cancel or disapply it. |
| Security | As with anything else sent over the internet, emails are not completely secure. There is no proof of receipt, emails can be 'lost', they can suffer from computer failure and a determined 'hacker' could intercept, read and possibly alter the contents.<br>As with other methods of written communication, you must make a judgment about the potential damage if the communication is lost or intercepted. Never send bank account information, including passwords, by email. |

| | |
|---|---|
| Program files and non-business documents | You must not introduce programme files or non-business documents from external sources on to the school’s network.<br>This might happen by opening an email attachment or by downloading a file from a website. Although virus detection software is installed, it can never be guaranteed 100 percent successful, so introducing nonessential software is an unacceptable risk for the school.<br>If you have any reason for suspecting that a virus may have entered the school’s system, you must contact the ICT support staff immediately. |
| Quality | Emails constitute records of the school and are subject to the same rules, care and checks as other written communications sent by the school. Emails will be checked under the same scrutiny as other written communications.<br>Staff members should consider the following when sending emails:<br>• Whether it is appropriate for material to be sent to third parties<br>• The emails sent and received may have to be disclosed in legal proceedings<br>• The emails sent and received maybe have to be disclosed as part of fulfilling an SAR<br>• Whether any authorisation is required before sending<br>• Printed copies of emails should be retained in the same way as other correspondence, e.g. letter<br>• The confidentiality between sender and recipient<br>• Transmitting the work of other people, without their permission, may infringe copyright laws.<br>• The sending and storing messages or attachments containing statements which could be construed as abusive, libelous, harassment may result in disciplinary or legal action being taken.<br>• Sending or storing messages or attachments containing statements which could be construed as improper, abusive, harassing the recipient, libelous, malicious, threatening or contravening discrimination legislation or detrimental to the is a disciplinary offence and may also be a legal offence. |
| Inappropriate emails or attachments | You must not use email to access or send offensive material, chain messages or list-servers or for the purposes of bullying or plagiarising work.<br>You must not send personal or inappropriate information by email about yourself, other members of staff, pupils or other members of the school community.<br>If you receive any inappropriate emails or attachments, you must report them to ICT support and/or DSL. |
| Viruses | If you suspect that an email has a virus attached to it, you must inform the ICT support staff immediately. |

| | |
|---|---|
| Spam | You must not send spam (sending the same message to multiple email addresses) without the permission of senior staff. |
| Storage | Old emails may be deleted from the school's server after 12 months.<br>You are advised to regularly delete material you no longer require and to archive material that you wish to keep. |
| Message size | Staff are limited to sending messages with attachments which are up to 10Mb in size. If you wish to distribute files within the school, you can do so by using the shared server. |
| Confidential Emails | You must ensure that confidential emails are always suitably protected. If working at home or remotely, you should be aware of the potential for an unauthorised third party to be privy to the content of the email.<br>Confidential emails should be deleted when no longer required. |

**Email policy – advice to staff**

Staff should remind themselves of the ICT Acceptable Use Policy which relates to the monitoring, security and quality of emails. In addition, staff should be guided by the following good practice:

- Staff should check their emails every working day and respond, as appropriate, within a reasonable period if the email is directly addressed to them.
- Staff should avoid spam, as outlined in this policy.
- Staff should avoid using the email system as a message board and thus avoid sending trivial global messages.
- Whilst accepting the convenience of the staff distribution list, staff should try to restrict its use to important or urgent matters.
- Staff should send emails to the minimum number of recipients.
- Staff are advised to create their own distribution lists, as convenient and appropriate.
- Staff should always include a subject line.
- Staff are advised to keep old emails for the minimum time necessary.

**Further guidelines**

- Remember – emails remain a written record and can be forwarded to others or printed for formal use.
- As a rule of thumb, staff should be well advised to only write what they would say face to face and should avoid the temptation to respond to an incident or message by email in an uncharacteristic and potentially aggressive fashion.
- Remember, "tone" can be misinterpreted on the printed page and once it is sent it could end up in the public domain forever. Email lacks the other cues and clues that convey the sense in which what you say is to be taken, and you can easily convey the wrong impression.
- Remember that sending emails from your school account is similar to sending a letter on school letterhead, so don't say anything that might bring discredit or embarrassment to yourself or the school.
- Linked with this and given the popularity and simplicity for recording both visual and audio material, staff are advised to remember the possibility of being recorded in all that they say or do.

For further information or to clarify any of the points raised in this policy please speak to the DPO.

## Appendix 1 – Staff ICT Acceptable Use Agreement

Whilst our school promotes the use of technology, and understands the positive effects it can have on enhancing pupils' learning and community engagement, we must also ensure that staff use technology appropriately. Any misuse of technology will not be taken lightly and will be reported to the headteacher in order for any necessary further action to be taken.

This acceptable use agreement is designed to outline staff responsibilities when using technology, whether this is via personal devices or school devices, on or off the school premises, and applies to all staff, volunteers, contractors and visitors.

Please read this document carefully, and sign below to show you agree to the terms outlined.

### Using technology in school

- I will only use ICT systems which have been permitted for my use by the headteacher, such as:
  - Computers.
  - Laptops.
  - Tablets.
- I will only use the approved email accounts that have been provided to me.
- I will not use personal emails to send and receive personal data or information.
- I will not share sensitive personal data with any other staff, pupils or third parties unless explicit consent has been received.
- I will ensure that any personal data is stored in line with the UK GDPR.
- I will delete any chain letters, spam and other emails from unknown sources without opening them.
- I will ensure that I obtain permission prior to accessing teaching materials from unapproved sources.
- I will only use the internet for personal use during out-of-school hours, including break and lunch times.
- I will not search for, view, download, upload or transmit any explicit or inappropriate material when using the internet.
- I will not share school-related passwords with pupils, staff or third parties unless permission has been given for me to do so.
- I will not install any software onto school ICT systems unless instructed to do so by the ICT lead or headteacher.
- I will ensure any school-owned device is protected by anti-virus software and that I check this on a weekly basis.
- I will only use recommended removable media and will keep this securely stored in line with the UK GDPR.
- I will only store data on removable media or other technological devices that have been encrypted of pseudonymised.
- I will only store sensitive personal data where it is absolutely necessary and has been encrypted.
- I will give removable media to the ICT lead for safe disposal once I am finished with it.

**Mobile devices**

- I will only use school-owned mobile devices for educational purposes.
- I will only use personal mobile devices during out-of-school hours, including break and lunch times.
- I will ensure that personal mobile devices are either switched off or set to silent mode during school hours, and will only make or receive calls in specific areas, e.g. the staffroom.
- I will ensure personal mobile devices are stored in a lockable cupboard located in the staffroom or classroom during lesson times.
- I will not use personal mobile devices to take photographs or videos of pupils or staff – I will seek permission from the headteacher before any school-owned mobile device is used to take images or recordings.
- I will not use mobile devices to send inappropriate messages, images or recordings.
- I will ensure that personal and school-owned mobile devices do not contain any inappropriate or illegal content.
- I will not access the WiFi system using personal mobile devices unless permission has been given by the headteacher or ICT lead.
- I will not use personal or school-owned mobile devices to communicate with pupils or parents.
- I will not store any images or videos of pupils, staff or parents on any mobile device unless consent has been sought from the individual(s) in the images or videos.
- In line with the above, I will only process images or videos of pupils, staff or parents for the activities for which consent has been sought.
- I will ensure that any school data stored on personal mobile devices is encrypted and pseudonymized, and give permission for the ICT lead to erase and wipe data off my device if it is lost or as part of exit procedures.

## 1. Social media and online professionalism

- If I am representing the school online, e.g. through blogging or on a school social media account, I will express neutral opinions and will not disclose any confidential information regarding the school, or any information that may affect its reputability.
- I will not use any school-owned mobile devices to access personal social networking sites, unless it is beneficial to the material being taught; I will gain permission from the headteacher before accessing the site.
- I will not communicate with pupils or parents over personal social networking sites.
- I will not accept 'friend requests' or 'follow requests' from any pupils or parents over personal social networking sites.
- I will ensure that I apply the necessary privacy settings to any social networking sites.
- I will not publish any comments or posts about the school on any social networking sites which may affect the school's reputability.
- I will not post or upload any defamatory, objectionable, copyright-infringing or private material, including images and videos of pupils, staff or parents, on any online website.
- I will not post or upload any images and videos of pupils, staff or parents on any online website without consent from the individual(s) in the images or videos.
- In line with the above, I will only post images or videos of pupils, staff or parents for the activities for which consent has been sought.

- I will not give my home address, phone number, mobile number, social networking details or email addresses to pupils or parents – any contact with parents will be done through authorised school contact channels.

**Working from home**

- I will adhere to the principles of the UK GDPR when working from home.
- I will ensure I obtain permission from the headteacher and ICT lead before any personal data is transferred from a school-owned device to a personal device.
- I will ensure any data transferred from a school-owned device to a personal device is encrypted or pseudonymised.
- I will ensure any sensitive personal data is not transferred to a personal device unless completely necessary – and, when doing so, that it is encrypted.
- I will ensure my personal device has been assessed for security by the ICT lead before it is used for lone working.
- I will ensure no unauthorised persons, such as family members or friends, access any personal devices used for lone-working.
- I will act in accordance with the school's Online Safety Policy when transporting school equipment and data.

**Training**

- I will ensure I participate in any online safety training offered to me, and will remain up-to-date with current developments in social media and the internet as a whole.
- I will ensure that I allow the ICT lead to undertake regular audits to identify any areas of need I may have in relation to training.
- I will ensure I employ methods of good practice and act as a role model for pupils when using the internet and other digital devices.
- I will ensure that I deliver any training to pupils as required.

**Reporting misuse**

- I will ensure that I adhere to any responsibility I have for monitoring, as outlined in the Online Safety Policy, e.g. to monitor pupils' internet usage.
- I will ensure that I report any misuse by pupils or staff members breaching the procedures outlined in this agreement to the headteacher.
- I understand that my use of the internet will be monitored by the ICT lead and recognise the consequences if I breach the terms of this agreement.
- I understand that the headteacher may decide to take disciplinary action against me, in accordance with the DDAT Disciplinary Policy and Procedure, if I breach this agreement.

---

I certify that I have read and understood this agreement, and ensure that I will abide by each principle.

Signed (**staff member**): Date:

Print name:

Signed (**headteacher**): Date:

Print name: