# Cleeve Prior CE Primary School

Cleeve Prior
CE PRIMARY SCHOOL

# Acceptable Use Policy 2024-25

# Contents:

## Our vision

Our vision is to provide a safe, caring and nurturing environment, where everyone is given opportunities to learn, discover and grow in our changing world. We will live out our Christian values of Respect, Hope, Love, Forgiveness, Trust and Honesty and strive to guide our community into leading fruitful lives, learning from Jesus' teachings, to love themselves and one another in order to achieve success. 'Teach children how they should live, and they will remember it all their life."

Proverbs 22:6

## Statement of intent

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 technology is used appropriately. Any misuse of technology will not be taken lightly and will be reported to the Head of School in order for any necessary further action to be taken.

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

## 1. Introduction

This policy applies to all employees, volunteers, supply staff and contractors using school ICT facilities.

The school acceptable use 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

This policy should be read in conjunction with the school's Data Protection Policy, Privacy Policy and Records Management Policy.

## 2. 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.

## Code of Practice for all Staff

| | |
|---|---|
| User ID and password and logging on | All staff and pupils will be given their own user ID and password. These must be kept private.<br>It is recommended that passwords 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 staff forget or accidentally disclose their password, they must report it immediately to a member of the ICT support staff.<br>Use of the school's facilities by a third -party using staff user name or password will be attributable to them, and the staff member will be held accountable for the misuse. |
| 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. Where possible, printing should be in black and white. |
| Logging off | Staff should log off from the computer they are using at the end of each session and wait for the standard login screen to reappear before leaving. |

| | |
|---|---|
| Access to information not normally available | Staff 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>Staff should 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 | Staff must not connect any hardware which may be detrimental to the school's network. |
| Connections to the computer | Staff should use the keyboard, mouse and any headphones provided. They must not adjust or alter any settings or switches without first obtaining the permission of the Head of School.<br>Staff may use USB memory sticks, or other portable storage media where a port is provided on the front or side of the computers.<br>Staff are not permitted to connect anything else to the computer without first getting the permission of the Head of School. |
| Virus | If staff suspect that their computer has a virus, they must report it to the Head of School immediately. |
| File space | Staff must manage their own file space by deleting old data rigorously and by deleting emails that you no longer require. |
| Reporting faults and malfunctions | You must report any faults or malfunctions in writing to the ICT support staff, including full details and all error messages, as soon as possible. |
| Copying and plagiarising | Staff must not plagiarise or copy any material which does not belong to them.<br>Any work crated on behalf of the school is the property of school and must remain on shared drive. |
| Copies of important work | 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. |

## 3. Internet policy and code of practice

The school can provide access to the internet from desktop PCs via the computer network and through a variety of electronic devices connected wirelessly to the network. Whenever accessing the internet using the school's or personal equipment staff 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 ICT staff.
- 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 for all staff

| | |
|---|---|
| Use of the internet | The Internet should not normally be used for private or leisure purposes; it is provided primarily for education or business use. Staff may use the internet for other purposes provided that:<br>● Such use is occasional and reasonable;<br>● Such use does not interfere in any way with their duties;<br>● Staff always follow the code of practice. |
| Inappropriate material | Staff 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>Staff are responsible for rejecting any links to such material which may appear inadvertently during research.<br>If staff encounter any material which could be regarded as offensive, they must leave that website or service immediately and not make any copy of that material. This should then be reported to the Head of School as soon as possible. |
| Misuse, abuse and access restrictions | Staff must not misuse or abuse any website or service or attempt to bypass any access controls or restrictions on any website or service. |
| Monitoring | The internet access system used by the school maintains a record which identifies who uses the facilities through the Smoothwall System.<br>The information collected includes which website and services are visited, how long staff remain there and which material is viewed. This information will be analysed and retained, and it may be used in disciplinary and legal proceedings. |
| Giving out information | Staff must not give any information concerning the school, its pupils 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 staff member's name when accessing a service which the school subscribes to. |
| Personal safety | All staff should take care with who you correspond with. Staff should not disclose where they are or arrange to meet anyone they do not personally know. |
| Hardware and software | Staff 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 | Staff 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. |

## 4. 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 for all staff

| | |
|---|---|
| • Purpose | Staff are only permitted to send a reasonable number of emails and should be work-related. |
| Monitoring | Copies of all incoming and outgoing emails, together with details of their duration and destinations are stored centrally (in electronic form).<br>The frequency and content of incoming and outgoing external emails may be checked to determine whether the email system is being used in accordance with this policy and code of practice.<br>The Head of School and technical staff are entitled to have read-only access to all emails. |
| 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, staff must make a judgment about the potential damage if the communication is lost or intercepted. |
| Program files and non-business documents | Staff must not introduce program files or non-business documents from external sources on to the school's network. 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 staff have any reason for suspecting that a virus may have entered the school's system, they should inform Head of School 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. |
| | 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, libellous, 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, libellous, 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 | Staff 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>Staff must not send personal or inappropriate information by email about themselves, other members of staff, pupils or other members of the school community.<br>If staff receive any inappropriate emails or attachments, they must report them to technical staff. |

| | |
|---|---|
| Viruses | If staff suspect that an email has a virus attached to it, they must inform the technical staff immediately. |
| Storage | Old emails may be deleted from the school's server after 12 months.<br>Staff are advised to regularly delete material they no longer require and to archive material that they wish to keep. |
| Confidential Emails | Staff must ensure that confidential emails are always suitably protected. If working at home or remotely, they should be aware of the potential for an unauthorised third party to be privy to the content of the email.<br>Wherever possible, the secure portal should be used for confidential messages.<br>Confidential emails should be deleted when no longer required. |

## 5. 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 daily 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 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.

## 6. Further guidelines

- 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.
- Staff should 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.
- Staff should 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 Data Protection Officer (Head of School).

Please sign below to confirm you have read and understood the school ICT Acceptable Use Policy:

Signed on behalf of school: ___________________________________________

Date: ___________________________________________

Signed by employee/volunteer/contractor/supplier:

___________________________________________

Date:

___________________________________________