Woolpit Primary Academy

NURTURE • RESILIENCE • INSPIRATION • RESPECT

Acceptable Use of ICT

January 2021

Reviewed By	Sarah Clayton
Signature	
Date	January 2021

Our vision:

Our core values are; **Nurture**, **Resilience**, **Respect**, **Inspiration**, which are at the heart of all we do. This is to ensure children leave Woolpit Primary Academy with a love of learning, as resilient individuals who are prepared for their futures. Our nurturing approach will ensure all pupils grow into well-rounded individuals with healthy minds. Children will leave our primary school as respectful members of the community; inspired to learn and motivated to achieve.

Table of Contents

1 INTRODUCTION 3

1.1 Purpose **Error! Bookmark not defined.**

1.2 Scope

2 RESPONSIBILITIES 3

2.1 Schools 3

2.2 Users 4

3 EMAIL 5

3.1 Email Etiquette 5

3.2 Legal Liability and Misuse of Email 6

3.3 Information Security, Viruses, Spam and Email Monitoring 6

4 PERSONAL USE AND PRIVACY 7

5 DATA 8

6 MOBILE PHONES, PHOTOGRAPHS AND INSTANT MESSAGING 8

7 SOCIAL NETWORKING 8

1 INTRODUCTION

The school recognises the important contribution that effective use of technology can make to learning, professional development and the efficient operation of the school. It encourages all members of the school community to make appropriate use of the available tools to learn, organise and share. However, there are risks and this policy seeks to provide clear guidelines to minimise them.

1.1 Purpose

1.1.1 The purpose of this policy is to:

- define and describe the acceptable use of ICT (including mobile phones and digital cameras) for the school, its staff, pupils and volunteers;
- minimise the risk to pupils of inappropriate use;
- minimise the risk to ICT systems and the information contained in them;
- to protect school governors and staff from litigation and disciplinary action;
- to describe the etiquette and standards that staff and pupils are expected to observe when using the school's email facilities and ensure that staff and pupils are aware of the consequences of inappropriate use;
- to provide clear guidance to staff, governors and volunteers on their use of social media in as far as it affects the school;
- ensure the reputation of the school is not adversely affected by inappropriate use of social media.

1.1.2 It is not the intention of this policy to impose restrictions that are contrary to a culture of openness and trust, and rights of access to information.

1.2 Scope

1.2.1 This policy applies to the use of ICT, websites, applications and email facilities for which the school is accountable and responsible. It is applicable to school governors, staff, pupils, and volunteers. It also includes partners and agents who the school has authorised to access ICT facilities including contractors and vendors with access to ICT systems. For the purposes of this policy all these individuals are referred to as 'user' or 'users'.

2 RESPONSIBILITIES

2.1 Schools

2.1.1 **Training** – The School will train users in the Acceptable Use of ICT (Schools), including health and safety requirements under the display screen regulations 1992, Information Security and Data Protection, including when it is appropriate and permissible to share data.

2.1.2 **Induction, Training and Support** – The School is responsible for ensuring that adequate induction and training is undertaken by users, including pupils, and that support is provided to them so as to implement this policy.

2.1.3 **User Access to Networks** – The Head Teacher, or delegated authority, is responsible for approving and authorising all user access to the School Network and ICT resources.

2.1.4 **Equipment Inventory** – The Headteacher is responsible for ensuring that an up to date inventory of ICT equipment is maintained together with a list of to whom it has been issued.

2.1.5 **System or Account Misuse** - When a complaint of possible system or account misuse by a user is reported, the validity of the incident will be reviewed by the Headteacher and advice sought from the County Education Officers who will agree an appropriate strategy for investigation.

2.1.6 **Equipment Disposal** - Equipment disposal will be managed in accordance with the *Waste Electrical & Electronic Equipment Directive (WEEE)*. Mobile Media (e.g. CD ROMS, DVDs) should be disposed of by way of shredding.

2.1.7 **Policy Development** – The Governing Body is responsible for reviewing the policy on an annual basis.

2.2 Users

2.2.1 **User Agreement** – By using the ICT equipment provided to them and by logging on to ICT or email systems, users agree to abide by this policy and any others that are relevant (eg. Safeguarding).

2.2.2 **Breach of Policy** – Staff found to be in breach of this policy may be disciplined in accordance with the school's disciplinary procedure. In certain circumstances, breach of this policy may be considered gross misconduct resulting in the termination of employment. Other users should be aware that breach of this policy may result in removal of school ICT access, pupil disciplinary action and, in certain circumstances, criminal investigation. Users must report all suspected breaches of this policy to the Headteacher.

2.2.3 **Training and Documentary Evidence** - All users should undergo appropriate training and ensure that they possess and supply all required documentary evidence (e.g. CRB).

2.2.4 **Access Authorisation** – Users must not connect, or attempt to connect, any ICT equipment provided to them to any network, or system; or access, or attempt to access, any network or system without prior explicit authorisation to do so.

2.2.5 **Data Protection** - All users are expected to act in a responsible, ethical and lawful manner with the understanding that electronic and manual information may be accessible to the public under the relevant information legislation, including the Freedom of Information Act 2000. Users should uphold privacy and confidentiality in accordance with the Data Protection Act 1998. Care must also be taken not to breach another person's copyright, trademark or design – nor to publish any defamatory content. Users responsible for managing data should follow current *School Policies and Procedures* and best practice. This includes specifying and taking appropriate measures to secure data from unauthorised access during normal working processes, in transit or when in storage. (See also the *Data* section)

2.2.6 **Authorised ICT Equipment** – Users must only attempt to access the schools network from authorised ICT equipment and systems.

2.2.7 **Inventory of ICT Equipment** - Users must inform the Headteacher if they change the location of any ICT equipment to ensure that it can be found easily.

2.2.8 **Mobile Devices** - Users allocated mobile devices (e.g. laptops, tablets, mobile phones, digital cameras) will be expected to sign for their receipt and must ensure that they are kept securely when not in use, or being transported and returned when they leave the school. The insurance policies used by the school do not cover loss of equipment from unattended vehicles. Staff may use school equipment for authorised business use only, except as allowed for in paragraph 2.3.2.

2.2.9 **Legal Responsibility** - No user may use ICT resources in violation of license agreements, copyrights, contracts or national laws, or the policies, rules or regulations of the school or County Council.

2.2.10 **Password and User Account Protection** - Users are required to use a secure password that could not be easily guessed. They must protect their password and not share their account details with others for their use, nor utilise another users' account or misrepresent their identity for any reason. Users must not log on to a machine using their password for another user to then use. Users must not under any circumstances reveal their password to anyone. Passwords used for school accounts must not also be used for any personal accounts.

2.2.11 **Access to Another User's Personal Electronic Documents** - No user shall access (e.g., read, write, modify, delete, copy, move) another user's personal electronic documents (including email) without the owner's permission or as allowed by this policy or by law. Personal electronic documents are those that are solely non business electronic documents.

2.2.12 **Unauthorised Access Protection** - Users must log out from or lock their PC or laptop when temporarily away from their desk to prevent unauthorised access and use a secure password. This applies wherever the user is located at the time of use (e.g. home or School). All pupil data must be stored in secure locations on the school network to which only authorised users have access.

2.2.13 **Access to Data** - Users must not access, load or download any data on any device without the knowledge, approval and authorisation of the owner and accountable person for the system the data originates from.

2.2.14 **Software and applications** – No user may load or download software on any device without the authorisation of the Headteacher. Periodic audits of software held on ICT equipment will be undertaken.

2.2.15 **Anti-Virus and Personal Firewall Software** - Network connected devices must have approved anti-virus and personal firewall software installed, activated and functioning. Users may not turn off anti-virus and personal firewall software. All users of ICT resources have the responsibility to take precautions to prevent the initial occurrence and subsequent spreading of a computer virus. No one may knowingly create, install, run, or distribute any malicious code (e.g. viruses, Trojans, worms) or another destructive program on any ICT resource. If a device is identified as being infected with a possible virus, Trojan or worm, steps will be taken to isolate it from the network immediately.

2.2.16 **ICT Security and Connection to Networks** - No one may knowingly or willingly interfere with the security mechanisms or integrity of ICT resources. No one may use ICT resources to attempt unauthorised use, or interfere with the legitimate use by authorised users, of other computers on internal or external networks. No one may make or attempt to make any unauthorised connection to the schools network or connect any computer, network system or other ICT device to the school network unless it has been approved by the school. Access to networks will be monitored as allowed for by this policy and law (see 2.3.6).

2.2.17 **Wireless Connections** – Users should not connect any School device to an unsecured Wireless Network.

2.2.18 **Inappropriate Material** - No one may use ICT resources to transmit abusive, threatening, or harassing material, chain letters, spam, or communications prohibited by law. No one may abuse the policies of any newsgroups, mailing lists, and other public forums through which they participate from a school account.

2.2.19 **Inappropriate Content** - The following content should not be created or accessed on ICT equipment at any time:

- pornography and “top-shelf” adult content;
- material that gratuitously displays images of violence, injury or death;
- material that is likely to lead to the harassment of others;
- material that promotes intolerance and discrimination on grounds of race, sex, disability, sexual orientation, religion, belief or age;
- material relating to criminal activity, for example buying and selling illegal drugs;
- material relating to any other unlawful activity e.g. breach of copyright;
- material that may generate security risks and encourage computer misuse.

2.2.20 **Accidental Access of Inappropriate Material or Content** - It is possible to access or be directed to unacceptable Internet sites by accident. These can be embarrassing and such sites can be difficult to get out of. If users have accessed unacceptable content or are in receipt of unacceptable material via email, they should inform the Head Teacher. This may avoid problems later should monitoring systems be alerted to the content.

2.2.21 **Website Blocking** - The school may block user access to various categories of websites, including download of content capability. This could be because the websites are not determined as appropriate for school use, or providing access could compromise the bandwidth of the Internet capability for essential school use, or that the content or download of content could pose a security threat to the school network. If there is a need to access or download content from a blocked website then the user requiring access must agree this with the Headteacher and request the access through the ICT technicians.

2.2.22 **Website Appropriate Access** - There may be circumstances where a website that would normally be blocked may not be because there is a legitimate need to access areas of the website, or download appropriate content. In these cases users must not access any areas of the site or download content for which there is not a legitimate need

2.2.23 **Personal Equipment –** Only school provided devices and tools should be used rather than personally owned equipment.

3 EMAIL

3.1 Email Etiquette

3.1.1 **Alternatives to Email** – Do not use email as the only method of communication. A face-to-face meeting or telephone conversation may be more suitable for complex or sensitive issues.

3.1.2 **Numbers of Emails –** People can feel overwhelmed by the number of emails they receive. Keep the use of email to a minimum.

3.1.3 **Proper English** – Maintain a concise, professional standard of communication using a standard font, proper grammar and make use of automatic spell checkers to ensure high standards are displayed.

3.1.4 **Freedom of Information Act** – any emails sent from a school email address could be made public under an FOI Act request. It is important, therefore, to include only facts and evidence-based opinions and to consider the consequences of any communication being made public.

3.1.5 **Personal and business content –** avoid mixing personal and business content within the same email.

3.1.6 **Email distribution** – Only distribute emails to colleagues or pupils who need to receive it. Avoid Reply to All unless genuinely needed. Avoid blind copying (bcc) unless sending to a large distribution list when it is both appropriate and necessary to hide individual email addresses to protect privacy. Users may only send emails to all parents or pupils if authorised to do so by the Headteacher.

3.1.7 **Email response –** do not assume a sent email has been read. Where possible, reply to emails promptly. Do not request "read receipts" by default.

3.1.8 **Large emails** – avoid sending emails with large attachments. It is better to upload such attachments to Google Docs and share them with colleagues as this avoids filling the recipient's mailbox.

3.1.9 **Mailbox Management –** Users are responsible for managing and deleting emails and maintaining email folders to ensure that mailboxes do not become full.

3.1.10 **Out of Office Messages –** Users who will not be using their email accounts due to absence should set a short out of office message and remove it immediately upon their return. Alternative contact details should be provided. Personal details about the reason for absence should not be included.

3.1.11 **Email Disclaimers –** Users should include a statement in email footers as follows:

"Emails sent to and from this school will be monitored in accordance with the law to ensure compliance with policies and to minimise any security risks.

The information contained in this email and any of its attachments may be privileged or confidential and is intended for the exclusive use of the addressee. Any unauthorised use may be unlawful. If you receive this email by mistake, please advise the sender immediately by using the reply facility in your email software."

3.2 Legal Liability and Misuse of Email

3.2.1 **Formal language –** Emails could commit the school to an agreement with parents, suppliers and other third parties, or provide evidence of harassment, defamation, libel and discrimination if worded incorrectly. The same care should be taken with them as with a formal letter.

3.2.2 **Personal Email Accounts –** Staff must not use a personal email account to send or receive school business emails. School accounts must not be set to forward automatically to a personal email account, although personal email accounts can be set to forward to a school account, although the school account has limited storage capacity and personal emails may have to be deleted if it fills up.

3.2.3 **Staff Emailing Pupils –** Staff must only email pupils or parents where there is a school need to do so.

3.2.4 **Users must not:**

- Use a false identity in emails nor use email for the creation or transmission of anonymous messages;
- Create emails, or alter a message and then forward it, with the intention of deceiving a recipient;
- Create, transmit, or forward any illegal, offensive, obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images;
- Create, transmit or forward material that is designed or likely to cause annoyance, inconvenience or needless anxiety;
- Create, transmit or forward material that is designed to or would conflict with the school business or undermine the school in any way;
- Create, transmit or forward emails containing staff, pupil or family personal information or information that is sensitive, to a personal or non-work email account of to a work email account where the recipient does not require it for legitimate use.

3.3 Information Security, Viruses, Spam and Email Monitoring

3.3.1 **Temporarily Away From Desk –** Staff and pupils must log out from or lock their PC when temporarily away from their desk to prevent unauthorised use of email accounts irrespective of location (home or school).

3.3.2 **Suspicious Activity –** Do not open any email from an unrecognised source or emails that have dubious or missing subject lines. Do not open unsolicited email attachments unless sure of the source. Disable the preview panel to minimise the risk of opening an infected email. Report any suspicious activity to the Headteacher or ICT support.

3.3.3 **Forwarding emails –** Never send or forward chain email messages or virus warnings. The vast majority are bogus and they waste time and network capacity. Do not forward material via email in breach of copyright.

3.3.4 **Inspection of email records –** Users must comply with a request from the Headteacher, or delegated authority, to inspect email records and/or to print out items relevant to a particular individual, case or subject. This will only be requested when required under the Data Protection Act, the Freedom of Information Act, as allowed for in section xxxx, or for other legitimate school business reasons. Deletion of emails by staff following such a request may be a criminal offence.

3.3.5 **Automatic Email Monitoring –** The school's email system will apply automatic message monitoring, filtering and rejection systems as appropriate and deny transmission or receipt of messages with content that represents a threat to the ICT network or is unacceptable in terms of this or other policies. Users granted administration privileges may examine messages placed in quarantine, and forward or delete them as appropriate.

4 PERSONAL USE AND PRIVACY

4.1.1 **Limitations of Personal Use** - In the course of normal operations, ICT resources are only to be used for school purposes. The school permits the personal use of ICT facilities and email services by authorised users subject to the following limitations:

- Personal use must be in the user's own time and must not impact upon the school efficiency or costs;
- The level of use must be reasonable and not detrimental to the main purpose for which the facilities are provided;
- Personal use must not be of a commercial or profit-making nature;
- The school's email system must not be used to send emails including adverts, sponsorship requests, appeals or details of events not supported by the school;
- Personal emails should be stored in a suitably marked folder in the user's inbox;
- Personal use must not be of a nature that competes with the business of the School or conflicts with an employee's obligations;
- It must not involve attempting to access the categories of inappropriate content in 2.2.19, even on a network outside school;
- Personal use must not bring the school into disrepute.

4.1.2 **Examples of Acceptable Personal Use** - Examples of acceptable personal use of ICT include online banking, shopping, learning activities, social networking (within the guidelines in section xx), access to news and weather websites and the use of software and email applications for personal organisation or charitable and other non-profit making activities.

4.1.3 **Recording and Inspecting Information** - Within the terms of the Data Protection Act 1998, Human Rights Act 1998 and the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, the School may record or inspect any information transmitted through or stored in its computers, including e-mail communications and individual login sessions, without notice when:

- There is reasonable cause to believe the user has violated, or is violating this policy, or any guidelines, or procedures established to implement this policy;
- An account appears to be engaged in unusual or unusually excessive activity;
- It is necessary to do so to protect the integrity, security, or functionality of ICT resources or to protect the School from liability;
- Establishing the existence of facts relevant to the business;
- Ascertaining or demonstrating standards which ought to be achieved by those using the ICT facilities;
- Preventing or detecting crime;
- Investigating or detecting unauthorised use of ICT facilities;

- Ensuring effective operation of ICT facilities;
- Determining if communications are relevant to the business (for example, in the last resort where an employee is off sick or on holiday and business continuity is threatened);
- It is otherwise permitted or required by law.

4.1.4 **Monitoring** - Any necessary monitoring will be carried out in accordance with the Information Commissioner's Office (ICO) *Code of Best Practice on Monitoring Employees*.

4.1.5 **Violation of this Policy** - Where an individual has reasonable cause to believe that another user has violated, or is violating this policy, or any guidelines, or procedures established to implement this policy then they shall in the first instance inform the Headeacher for investigation under the school's policies and procedures. In certain circumstances the checks may necessitate the immediate suspension of the user's access to the School Network, ICT resources, ICT systems and applications in order that any potential evidence is not compromised.

5 DATA

5.1.1 **Managing Data** - Users responsible for managing data should follow best practice. This includes specifying and taking appropriate measures to secure data from unauthorised access during normal working processes, in transit, when in storage or in the possession of third parties.

5.1.2 **'Sensitive' or Protectively Marked Data** - Where the user is accessing a system showing 'sensitive' data then the screen must not be easily readable by anyone other than the logged-in user. Workstations and screens shall be arranged to ensure that the screen is facing away from the line of sight of any visitors.

5.1.3 **Personal Documents and Folders** - Personal documents and folders regarded as "personal" must be clearly titled to reduce the risk of administrators inadvertently viewing private, non-work documents. Personal documents and folders must be deleted from the School systems as soon as possible.

5.1.4 **Printed Material** – Users must securely store or destroy any printed material.

5.1.5 **Movement of Data and Records** – Users must not remove information (data and records both electronic and paper) from School premises without appropriate approval.

6 MOBILE PHONES, PHOTOGRAPHS AND INSTANT MESSAGING

6.1.1 **Numbers** – Staff should not give their home telephone number or their mobile phone number to pupils or parents/carers, unless this has been authorised for a specific purpose by the Headteacher. They should not use pupils' mobile phone numbers to communicate with pupils unless specifically authorised by the Headteacher for school business.

6.1.2 **Photographs** –

- Photographs and videos of pupils must not be taken on personal mobile devices.
- Only school cameras are to be used to take photographs and videos in school.
- No personal cameras are to be used without the written permission of the Headteacher.
- Photographs must be stored on the school network or the school's online photo account (Picasa). They may only be downloaded onto hard drives for the completion of a school project and must be deleted when complete.
- Voluntary helpers and parents must not take photographs on their own cameras during school trips.
- Students and work experience students must not take photographs without the written permission of the Headteacher.

6.1.3 **Electronic communication with pupils** – staff must only use school accounts to communicate electronically with pupils and only for approved school purposes, eg. Homework.

6.1.4 **Instant Messaging** – staff may not communicate with pupils by instant message unless this is part of a lesson.

7 SOCIAL NETWORKING

7.1.1 **Benefits** – The school recognises that staff, governors and volunteers have a right to use social media for personal purposes and that online networks can be of great value in professional development. Online social media sites can also be excellent tools for teaching and learning and can provide exciting, new opportunities for schools to engage, communicate and collaborate with pupils and the wider community. The positive use of social media and ICT within schools and settings for curriculum and learning is encouraged.

7.1.2 **Risks** – Social networking and media sites can have risks. They have changed how we communicate and this can lead to people posting unsafe or inappropriate information about themselves and their personal lives online as well as providing opportunities for offenders to groom and abuse children. This guidance seeks to ensure that activity in social media does not put the school, its staff or pupils at risk.

7.1.3 **Scope** – social media sites include, but are not limited to, Twitter, Facebook, YouTube, Flickr, Tumblr as well as blogs, forums, wikis and websites that allow public comments.

7.1.4 **General guidelines:**

- Users must not make any derogatory, defamatory, rude, threatening or inappropriate comments about the school, or anyone at or connected with the school.
- Users must ensure that neither their personal/professional reputation, nor the school's reputation is compromised by inappropriate posting.
- Users must not use of the school's name, logo, or any other published material without prior permission from the Headteacher.
- Users must not disclose confidential information or anything that could compromise the security of the school (eg. The delivery of expensive new equipment).
- Users must never post anything online that allows individual children or classes to be identified and must not post images of children, employees, governors or volunteers engaged in school activities unless specific permission has been given by the individual and Headteacher.
- Users must be aware that even on apparently "private" forums, online postings are effectively public and cannot be deleted.
- Staff must not accept requests from current school parents as "friends" on social network sites.
- Users should observe these rules even if posting on an anonymous or pseudonymous account because of the risk of exposure.

7.1.5 **Use in and by the school**

- No use of social media is permitted for school purposes without the specific permission of the Headteacher.
- A risk assessment should be undertaken of any social media application prior to its use.
- Pupils must never disclose their full names, email addresses or any information that would allow them to be identified.
- All parents of pupils involved in social media use should have signed xxxx agreeing to the use of xxx
- All posts to school social media sites must be moderated by an authorised adult before publication.
- All pupils should be clearly reminded before each use of social media, including email, to report any inappropriate content or messages seen or received online. Such instances should be reported promptly to the headteacher who will decide if the issue is serious enough to prompt further action.