Westwood Primary School

E-Safety & Acceptable Use of the Internet, Use of ICT and Mobile Phones Policy

E Safety and Acceptable use of the Internet

Safe use of computers and the Internet is promoted at our school. All staff and responsible adults are given guidance to ensure they have appropriate skills and understanding to teach the children. Age appropriate information is given to children at the beginning of the school year as part of each teacher's work with their new class regarding roles and responsibilities. Using computers in a safe way is part of the wider PSHE provision of how to look after ourselves and the school's legal responsibility to keep children and staff safe.

How we ensure use of the internet is as safe as possible in school

A service is provided to the school by Suffolk County Council which filters our access to certain sites on the Internet and blocks known threats. All reasonable action has therefore been taken by the school to avoid exposure to unsuitable material available on the Internet. However staff and parents must be aware that the Internet is a relatively ungoverned entity and it cannot be guaranteed that all sites deemed unsuitable will be blocked at all times as the World Wide Web grows daily.

The internet is a communications medium and is freely available to any person wishing to send e-mail or publish a web site. In common with other media such as magazines, books and video, some material on the internet is unsuitable for pupils. Pupils in school are unlikely to see inappropriate content in books due to selection by publisher and teacher and the school will take every practical measure to ensure that children do not encounter upsetting, offensive or otherwise inappropriate material on the internet.

As a school we feel that in the 21st Century access to computers and the Internet as a tool for research and work is essential and indeed a statutory requirement providing all reasonable measures are in place to make it as safe and enjoyable as possible.

Staff Responsibilities

Staff are expected to remain professional at all times and are provided with access to ICT equipment, the Internet and e-mail as standard. They are therefore expected to:

- Ensure all adults working with the children in their class are conversant with the school's policies and procedures regarding safe use of ICT equipment.
- Ensure children are informed of rules and responsibilities regarding safe and proper use of ICT equipment at the beginning of each academic year and reminded periodically by referring to the rules displayed in the ICT suite and classrooms.
- Protect their unique username and password access to the system by always locking any computer they are logged in to when unattended and logging out promptly
- Maintain appropriate professional conduct when using social networking and/or e-mail services. Refer to Code of Conduct Policy.
- School staff should not use email or social networking sites to contact children or parents. Any email contact should be via a school account and only related to curriculum matters.
- Staff must not use mobile phones for taking or passing on or publishing photos of children or school activities.
- **If a member of staff or adult in school sees anything on the school network or internet that upsets or offends they should report this straightaway to the Headteacher**

Children's Responsibilities:

Children are expected to follow the rules and responsibilities as outlined by their teacher and any responsible adults within the school. They should understand they are designed to keep them safe when using the Internet and ensure they use all ICT equipment effectively.

They are expected to:

- Follow instructions given to them by their teacher or responsible adult.

Rules for Being Safe on the Internet: SMART

These rules are to be displayed where there is access to computers (i.e. ICT suite, classrooms, laptop trolleys, etc)

S Stay **SAFE** by not giving out personal information online.

M **MEETING** someone who you only know online can be dangerous.

A **ACCEPTING** emails, pictures or texts from unknown people can be risky.

R Not all information you find online might not always be **RELIABLE** or true.

T **TELL** an adult in school, parent, carer or trusted adult if something or someone online makes you feel uncomfortable.

Discrimination and Harassment: For all school staff and children

As in our Equalities and Anti-Bullying Policy we do not tolerate discrimination, harassment or bullying of any kind. You must not use school ICT equipment or e-mails to spread any materials that are discriminatory, harass others, are prejudiced against ethnic or religious groups, and are intolerant of sexual orientation or derogatory about disability.

Of course any behaviour on the internet that is intentionally meant to bully will be dealt with through the anti-bullying policy and disciplinary procedures.

Parental Responsibilities

We hope parents and carers at home will continue the school's good work by promoting safe and proper use of the Internet and e-mail.

Parent's can help their children and the school as follows:

- Following the same rules at home as the children are expected to at school. Parents need to be aware that their home Internet access may be completely unrestricted and their children will have access to a far greater variety of information and websites.
- Instil the ethos of e-safety in an age appropriate way to ensure children understand the possible dangers of using social networks, e-mail and the Internet to browse for information and/or contact any unknown persons.

School responsibilities;

To minimise the risks of problems with using the internet and to promote e-safety:

1. Clear rules for everyone in school on safe use.
2. Use the County Council provided internet service with a 'firewall' that is designed to prevent access to inappropriate material.
3. We will ensure that all networked computers have regular updates of anti-virus software to minimise the risk to users.
4. All users in school except children in Early Years have separate usernames and passwords.
5. The IT technician and subject co-ordinator will occasionally check the system log for any inappropriate use and log this monitoring. Any inappropriate use will be addressed and if necessary disciplinary measures taken.
6. Consent for children to access the internet will be gained from parents / carers annually.
7. We will not publish any children's full names on any website or with their photos on any website.

Acceptable Use of ICT and Mobile Phones Policy

- The Governing Body is responsible for ensuring that its employees act in a lawful manner, making appropriate use of school technologies for approved purposes only.

- The Governing Body is responsible for adopting relevant policies and the Headteacher responsible for ensuring that staff are aware of their contents.

- The Headteacher is responsible for maintaining an inventory of SCT equipment and a list of school laptops and mobile phones and to whom they have been issued.

- If the Headteacher has reason to believe that any ICT equipment has been misused, he/she should consult the Area Personnel Officer or Education Lead Officer at the Area Office for advice without delay. The Area Personnel Officer will agree with the Headteacher and CSD's Policy and Compliance Manager an appropriate strategy for the investigation of the allegations. Incidents will be investigated in a timely manner in accordance with agreed procedures.

- Staff found to be in breach of this policy may be disciplined in accordance with the disciplinary procedure.

User Responsibilities

- Users and their managers are responsible for ensuring that adequate induction, training and support is undertaken to implement this policy.

- By logging on to ICT systems, users agree to abide by this Acceptable Use policy and other policies that relate to the use of ICT.

- All users are expected to act in a responsible, ethical and lawful manner with the understanding that school electronic and manual information may be accessible to the public under 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.

- Staff who have been given the use of a school laptop will be expected to sign for its use on receipt. Staff may use school equipment for authorised business use only, except as allowed

- Staff must follow authorised procedures when relocating ICT equipment or taking mobile devices offsite.

- No one may use ICT resources in violation of license agreements,copyrights, contracts or national laws, or the Standing Orders, policies, rules or regulations of the school or the County Council.

- Users are required to 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 riot under any circumstances reveal their password to anyone else.

- 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.

- Users must not load or download software on any device without the authorisation of the Headteacher. Periodic audits of software held on ICT equipment will be undertaken.

- Users must take care to store sensitive information, e.g. pupil data, safely and to keep it password protected, on all school systems, including laptops.

- Network connected devices must have school approved anti-virus software installed and activated. Users may not turn off anti-virus 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.

- No one may knowingly or willingly interfere with the securitymechanisms 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. Access to networks will be monitored.

- 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 County Council or 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, 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 County Council or its partners 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.

- Do not send private, sensitive or confidential information by unencrypted email - particularly to an external recipient - if accidental disclosure could lead to significant harm or embarrassment. Anonymise personal data where possible e.g. by using initials. Use passwords on sensitive documents that must be sent to external recipients.
- Websites should not be created on school equipment without the written permission of the Headteacher.
- 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.
- 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 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
- 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 staff have accessed unacceptable content or are in receipt of unacceptable material via email, they should inform the Headteacher. This may avoid problems later should monitoring systems be alerted to the content.

INFORMATION MANAGEMENT AND SECURITY

- User passwords are changed regularly and every time staff who have knowledge of passwords leave the employment of the school.

- Staff do not leave a work station having access to personal data unattended without locking the workstation or logging off from the network/machine.
- Laptops and other ICT equipment are not left unattended in vehicles
- Laptops should not have personal data stored on them unless encryption software is in operation.
- Staff must not send emails or attachments that contain personal data unless it is encrypted.
- Any printouts of personal and sensitive data should be kept securely and disposed of appropriately when no longer required.
- Personal data is not stored on mobile storage devices (USB storage devices, CDs, DVDs, etc.) unless encrypted
- Bulk transfer of personal data is only sent to third parties using secure protocols e.g. AnyComms
- Administration and financial databases are backed up frequently and Server and PC backup tapes/disks are stored in a fire proof safe.
- Wireless Networks have WPA encryption as a minimum

PERSONAL USE & PRIVACY

- In the course of normal operations, ICT resources are to be used for business purposes only. The school permits limited personal use of ICT facilities by authorised users subject to the following limitations:
    - Personal use must be in the user's own time and must not impact upon work 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.
    - Personal use must not be of a nature that competes with the business of the school or conflicts with an employee's obligations.
- Personal use of the Internet must not involve attempting to access the categories of content described in section 4.18 that is normally automatically blocked by web filtering software.

ICT RECOVERY PLAN

- Backups of management information should be carried out regularly at least once a week

- Updated copies of backup to be kept off site

- Details of ICT licenses should be stored in a fireproof safe

Use of Mobile Phones

- Staff should not give their home or mobile telephone number to pupils.
- Staff should not use their own personal mobile phones to phone or email parents.
- Photogrpahs and videas of pupils should not be taken with mobile phones
- Staff should not have a pupils of parent's mobile phone number either to make or receive phoneclas, or etxt messages or have numbers stored intheir phone.
- Staff should only communicate with pupils and parents from school accounts on approved school business
- Pupils should not enter into social networking or instant messageing communictaions with pupils or parents.

DISPOSAL OF ICT EQUIPMENT

- The Waste Electrical and Electronic Equipment (WEEE) directive is followed. All electrical equipment is disposed of according to the Directive and is not thrown away in general rubbish. Redundant equipment must not be given to third parties or to staff or pupils.

- All hard drives must be wiped before disposal.

- Correct certification will be collected by the school office.