Stanton Community Primary School

Nurture, Enjoy, Aspire, Achieve

Acceptable Use of ICT and Mobile Phones Policy

PURPOSE
The policy defines and describes the acceptable use of ICT (Information and Communications Technology) and mobile phones for school-based employees and volunteers. Its purpose is to minimise the risk to pupils of inappropriate contact from staff and volunteers, to protect employees and schools from litigation and to minimise the risk to ICT systems.

SCOPE
This policy deals with the use of ICT facilities in schools in Suffolk and applies to all school- based employees and other authorised users, e.g. volunteers.

Non-school based staff are subject to the Suffolk County Council's ICT Acceptable Use Policy.

SCHOOL RESPONSIBILITIES
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 Head Teacher for ensuring that staff are aware of their contents.

The Head Teacher is responsible for maintaining an inventory of ICT equipment and a list of school laptops and mobile phones and to whom they have been issued.

If the Head Teacher 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 Head Teacher an appropriate strategy for the investigation of the allegations. Incidents will be investigated in a timely manner in accordance with agreed procedures.

Head Teachers should make it clear that internal school staff should not carry out any investigations unless they are both qualified and authorised to do so.

USER RESPONSIBILITIES
Staff found to be in breach of this policy may be disciplined in accordance with the disciplinary procedure. In certain circumstances, breach of this policy may be considered gross misconduct resulting in termination of employment. Users must report all suspected breaches of this policy to the Head Teacher.

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 for in paragraph PERSONAL USE & PRIVACY.

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 not 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 Head Teacher. 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 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. 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. If there is accidental disclosure of personal, sensitive or confidential information the school DPO must be notified within 72 hours. The school DPO is Sian Durrant on data.protection@schoolschoice.org.

Websites should not be created on school equipment without the written permission of the Head Teacher.

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 Head Teacher. This may avoid problems later should monitoring systems be alerted to the content.

USE OF YOUTUBE AS A TEACHING TOOL

The school acknowledges that YouTube is designed for users aged 13 years old and above therefore all school devices (laptops and tablets) with exception of the teacher laptops have had access to the YouTube website removed.

The school acknowledges that YouTube is a useful teaching tool and therefore teachers must take the following approach when researching and showing material in class:

- Searches, or first observations of a potential video, should not be carried out with any child in the classroom. Once staff have finished watching their chosen video, it is imperative that the browser is closed down which will then ensure that YouTube cannot be accessed by children.
- Before showing a video to the class, the video should be watched and listened to carefully by the class teacher or TA. While watching they should look out for inappropriate content or material, along with any inappropriate comments that appear underneath the video.
- It is the class teacher's responsibility to make the final approval of a video.
- Teachers should also be aware of the advertisement on YouTube videos and these should be watched before showing the video to the children, without any children in the classroom. Advertisements can be shown at the start or during any video on YouTube. To ensure these do not show while using the video during the lesson, teachers must watch the video fully before any children enter the classroom. Once this has been done, the teacher can then show the video in full from the beginning.
- When the video is finished, the Smartboard should be frozen, stilled or muted (or even turned off) so that the video can be exited and the YouTube window can be closed safely.

When planning lessons, if a YouTube video is found that would broaden the context of a subject being taught in class, but may have an age rating that is above the age range of the class that is being taught, then parental approval will be sought before showing the video to the class.

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 that is normally automatically blocked by web filtering software.

MOBILE PHONE COMMUNICATION AND INSTANT MESSAGING

Staff are advised not to give their home telephone number or their mobile phone number to pupils or parents. Mobile phone communication should be used sparingly and only when deemed necessary.

Photographs and videos of pupils should not be taken with personal mobile phones.

Staff are advised not to make use of pupils' mobile phone numbers either to make or receive phone calls or to send to or receive text messages from pupils.

Staff should not enter into instant messaging communications with pupils. Class Dojo can be used to message parents and reply to their messages. However, these messages should only relate to school business.

This policy should be read in conjunction with:

- Bring Your Own Device Policy
- Data Protection Policy
- Information Management Handbook
- Child Protection and Safeguarding Policy
- Online Safety Policy
- Social Networking Policy
- Staff Code of Conduct
- Governors Code of Conduct

This policy should be reviewed annually.

Policy reviewed: January 2019

May 2018
To be revised January 2020