Carlton Colville Primary School

What we learn with pleasure we never forget

Acceptable Use of ICT and Mobile Phones Policy (also see Policy/guidance on the use of Social Networking sites, Photography and Video Policy)

1. PURPOSE

The Acceptable Use Policy (AUP) sets out the roles, responsibilities and procedures for the acceptable, safe and response use of all Information and Communication technologies (including the internet, email, webcam, social networking, mobiles and games) to safeguard adults and children within the school.

The policy is designed to protect users and explains the procedures for any unacceptable or misuse of these technologies by adults or children.

2. SCOPE

a) This policy deals with the use of ICT facilities/equipment in schools in Suffolk and applies to all school-based employees users including, but not limited to: school governors, staff, volunteers and other authorised users.
b) Non school-based staff are also subject to the County Council's ICT Acceptable Use Policy.

3. TRAINING

All staff will receive training regarding this policy (including any amendments) and any new staff and volunteers will receive this training as part of their induction.

4. SCHOOL RESPONSIBILITIES

a) 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.

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

c) The Headteacher is responsible for maintaining an inventory of ICT equipment and a list of school laptops, DVD Camcorders and mobile phones and to whom they have been issued.

d) 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.

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

f) The Headteacher should ensure that the AUP is reviewed annually.

g) The Headteacher should ensure all staff sign the Acceptable Use Statement.

h) The ICT co-ordinator should ensure that there is appropriate and up-to-date antivirus software and anti-spyware on the network, stand-a-lone PC's and teacher/child laptops and that this is reviewed and updates on a regular basis.

i) The ICT co-ordinator should ensure that the Internet filtering is set to the correct level for staff and children.

5. STAFF RESPONSIBILITIES

a) 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 Headteacher.

b) 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.

c) 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.

d) 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.

e) Staff must follow authorised procedures when relocating ICT equipment or taking mobile devices offsite. School cameras should not be used for personal use.

f) 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.

g) 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. Passwords are changed regularly and every time staff who have knowledge of the passwords leave the employment of the school.

h) 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.

i) Users must log out or lock their PC/Laptop when away from their desk to prevent unauthorised access. This applies wherever the user is located (home or school).

j) 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.

k) Users must take care to store sensitive information, e.g. pupil /finance data safely and to keep it password protected, on all school systems/encrypted memory sticks and laptops.

l) Laptops and other ICT equipment (e.g. Digital Cameras/DVD Camcorders/Memory Sticks) should not be left in unattended in a public place including items locked securely in an unattended vehicle.

m) Users should not connect any school equipment to an unsecured wireless network i.e. Public domains.

n) 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.

o) 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.

p) 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.

q) 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.

r) External websites (accessible by the public) should not be created on school equipment without the written permission of the Headteacher.

s) 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.

t) 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
- Any other material that could have a negative impact on the safety and wellbeing of children and young people.

u) 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.

6. USE OF SOCIAL NETWORKING SITES

The use of social networking sites by pupils on school computers is not permitted and access is blocked via the internet filtering service. The use of social networking sites outside of work hours is the personal choice of all staff. Owing to the public natures of such websites, it is advisable for staff to consider the possible implications of participation. The following advice should be involved in social networking:

- Staff should ensure that all possible privacy settings are activated to prevent pupils from making contact on personal profiles. The simplest and most effective way to do this is to remove details from search results and turn off public visibility.
- Staff should not engage in personal online contact with pupils outside of Headteacher authorised systems, eg school email account for homework purposes. Staff should not be 'friends' to pupils on a social networking site. It is also extremely advisable not to accept as friends ex-pupils who are still minors. If any pupil makes contact with staff as per the above, they must decline the request and notify the Senior Designated Professional (SDP) as soon as possible. The SDP can then deal with the situation as appropriate.

- Staff should ensure that full privacy settings are in place to prevent students from accessing photo albums or personal information. Facebook setting should be set to friends only (using friends of friends is not secure and may lead to pupils and parents having access to postings).
- Staff are advised against accepting invites from colleagues until they have checked with them in person that the invite is genuine (avoiding fake profiles set up by children).
- Staff must not post material (including text or images) which damages the reputation of the school or which causes concern about their suitability to work with children.
- Staff should not place any details relating to their professional life on any personal or social websites. Those who post material which could be considered as inappropriate could render themselves vulnerable to criticism or allegations of misconduct.
- Staff should be aware that any comments published on such sites which are deemed to be defamatory may result in an individual facing an expensive legal claim by the person wronged.
- Personal profiles on social networking sites or blogs should not identify your employer; the information you post could be considered to bring your school or organisation into disrepute and as such could lead to disciplinary action. The employer box should be left empty, Suffolk County Council should not be used as an alternative to the school name.
- Staff are advised not to place personal or confidential information on social websites as such information may be accessed by strangers and once published, eg photographs, blog posts etc is impossible to control and may be manipulated without your consent, used in different contexts or further distributed.

7. PUPIL RESPONSIBILITY

a. Children are responsible for following the Acceptable Use Rules whilst within school as agreed at the beginning of each academic year or whenever a new child attends the school for the first time.

b. Children are taught to tell an adult about any inappropriate material or contact from someone they do not know straight away, without reprimand (age and activity dependant).

c. Children are taught not to disclose their username or password to anyone nor should they leave a computer or other device unattended whilst they are logged in.

d. When accessing the schools emails from home, the same AUP apply.

8. RESPONSIBILITY OF PARENTS AND CARERS

a. Each child will receive a copy of the AUP on an annual basis or first-time entry to the school which need to be read with the parent/carer, confirming both an understanding and acceptance of the rules. Parents who have concerns or do not accept the rules should contact the school in writing to ensure their child does not have access to ICT. It is expected that parents/carers will explain and discuss the rules with their child (potentially enforcing the rules at home) so they are clearly understood and accepted.

9. PERSONAL USE & PRIVACY

a. 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.

b. Personal use of the Internet must not involve attempting to access the categories of content described in section 4.T that is normally automatically blocked by web filtering software.

10. ICT RECOVERY PLAN

a) Back ups of management information should be carried out regularly, at least once a week.
b) Updated copies of back up to be kept off site.

c) Details of ICT Licenses should be stored securely and a photocopy kept offsite.

MOBILE PHONE COMMUNICATION AND INSTANT MESSAGING

- Pupils are not permitted to use mobile phones within school and devices must be turned off at the school gate and handed into the teacher at the start of the school day.

- Unless there is an emergency, staff are expected to only access their mobile phones for personal use outside working hours.

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

- Photographs and videos of pupils should not be taken with 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 from pupils text messages other than for approved school business.

- Staff should only communicate electronically with pupils from school accounts on an approved Learning Platform, e.g. Topic work/Home-learning.

- Staff should not enter into instant messaging communications with pupils.

- Staff will use the agreed Teachers2Parents Text Messaging Service when appropriate.

12. USE OF GAMING PLATFORMS AND WEARABLE TECHNOLOGY

- The use of gaming platforms by staff or pupils is not permitted within school without the written consent of the Head Teacher.

- The use of wearable technology by pupils is not permitted.

- Within school, staff may only use wearable technology outside of working hours. The use of such technology must not breach any of the previously stated rules on accessible content (paragraph 5f) and must not be connected to the school's network.

13. USE OF PHOTOGRAPHS IN SCHOOL

- Photos will be taken with school cameras only and downloaded only onto school computers/laptops;
- Parental permission will be obtained before publication of any photos on external websites or in newspapers. Failure to obtain consent could result in formal action being taken;
- Children will be identified by first names only when pictures are published;
- Staff will check school records for photo permission slips before publishing photos on the school website.

14. PROCEDURES FOLLOWING MISUSE BY STAFF

The Headteacher will ensure that these procedures are followed, in the event of any misuse of the ICT by an adult:

a) An inappropriate website is accessed inadvertently:
Report website to the ICT Co-ordinator so that it can be added to the banned or restricted list.

b) An inappropriate website is accessed deliberately:
Ensure that no-one else can access the material by shutting down. Report to the Headteacher immediately and inform the ICT Co-Ordinator so that it can be added to the banned or restricted list.

c) An adult receives inappropriate material:
Do not forward this material to anyone else – doing so could be an illegal activity. Alert the Headteacher immediately. Ensure the device is removed and log the nature of the material. Contact relevant authorities for further advice, eg police.

d) An adult has used ICT equipment inappropriately:
Follow the procedures for b).

e) An adult has communicated with a child or used ICT equipment inappropriately:
    - Ensure the child is reassured and remove them from the situation immediately if necessary. Report to the Headteacher and Designated E-Safety Co-ordinator immediately. Preserve the information received by the child if possible and determine whether the information received is abusive, threatening or innocent.

- Once Procedures and Policy have been followed and if the incident is considered innocent, refer to the Acceptable Use Rules for Staff and Headteacher to implement appropriate sanctions.
- If illegal or inappropriate use is known, contact the Headteacher, Deputy Headteacher or Chair or Governors (if allegation is made against the Headteacher) and Designated Person for Safeguarding immediately and follow the Allegations procedure and Safeguarding Policy.
- Contact CEOP (police) as necessary.

f) Threatening or malicious comments are posted to a website or learning platform (or printed out) about an adult in school:

Preserve any evidence. Inform the Headteacher immediately and follow Safeguarding Policy as necessary. Contact the police or CEOP as necessary.

15. **PROCEDURES FOLLOWING MISUSE BY CHILDREN**

The Headteacher will ensure that these procedures are following in the event of any misuse or the internet by a child:

a) An inappropriate website is accessed inadvertently:

Reassure the child that they are not to blame and praise the child for being safe and responsible by telling an adult. The class teacher should inform the child's parents/carer and reassure them that the matter will be dealt with.

Report website to the ICT Co-ordinator who will add it to the banned or restricted list.

b) An inappropriate website is accessed deliberately:

Refer the child to the Acceptable Use Rules that were agreed. Reinforce the knowledge that it is illegal to access certain images and police can be informed. Decide on appropriate sanction. Notify the parent/carer.

c) An adult or child has communicated with a child or used ICT equipment inappropriately:

Ensure the child is reassured and remove them from the situation immediately. Report to the Headteacher or designated Person for Safeguarding immediately. Preserve the information received by the child if possible and determine whether the information received is abusive, threatening or innocent.

If illegal or inappropriate misuse the Headteacher must follow the Allegation Procedure and/or Safeguarding Policy. Contact CEOP (police) if necessary.

d) Threatening or malicious comments are posted to the school website or learning platform about a child in school:
Preserve any evidence. Inform the Headteacher and ICT Co-ordinator immediately. Contact the police or CEOP as necessary.

e) Threatening or malicious comments are posted on external websites about an adult in the school by a child:
Preserve any evidence. Inform the Headteacher immediately.

16. GENREAL ADVICE FOR ALL INSTANCES OF MISUSE

N.B. There are three incidences you must report directly to the police:

- Indecent images of children found
- Incidents of 'grooming' behaviour
- The sending of obscene materials to a child.

CEOP advice is to turn off the screen, secure the machine and contact the police for further instructions if an indecent image is found. Equipment suspected of being involved with inappropriate use cannot be used by anyone, should be clearly identified, stored securely and only CSD ICT staff or the police should be given access to carry out any investigation.
They will advise on how to deal with the machine, if they are unable to send out a forensics team immediately. If in doubt, DO NOT power down the machine.
Grabbing a screenshot is not a technical offence of distribution, but of 'making an image'.
www.iwf.org.uk will provide further support and advice in dealing with offensive images on-line.
It is important to remember that any offensive images that may be received should never be forwarded to anyone else, even if it is to report them as illegal, as this constitutes illegal activity and you will be liable to prosecution and investigation by the police.

LINKS TO OTHER USEFUL POLICIES

This policy should be read in conjunction with the:

- Safeguarding Policy
- Online-Safety Policy
- Whistle-blowing Policy
- Code of Connections and Information Security Policy
- ICT Policy
- Suffolk County Council Acceptable ICT Use Guidance for Staff and Managers.

Include copies of staff and pupil user agreements.

To be reviewed annually.

Date Reviewed: July 2016 – Amended January 2017

Review Date: July 2017