St Edmundsbury and Ipswich
Diocesan Multi Academy Trust

Hartest CE Primary School

Acceptable Use of ICT and Mobile Phones Policy

HARTEST SCHOOL

Prepared By	*Matthew Coombs* *Headteacher*
Approved by the Committee/Governing body	*LGB – Hartest CE Primary School*
Signature of Chair of Governors	
Date Approved	*January 2020*
Review Date	*January 2022*

Acceptable Use of ICT and Mobile Phones Policy

1 PURPOSE

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

2 SCOPE

This policy deals with the use of ICT facilities in schools in Suffolk and applies to all school-based employees, governors and other authorised users, e.g. volunteers. This policy should be read in conjunction with the schools Safeguarding and Online Safety Policies.

3 SCHOOL RESPONSIBILITIES

3.1 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.

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

3.3 The Headteacher 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.

3.4 If it is suspected that a member if staff, an adult or pupil has been misusing the school's computer equipment or accessing inappropriate websites or materials the Headteacher / DSL should inform the Local Authority Designated Officer or Area Manager immediately (reporting procedures as per school's Safeguarding Policy). There must be no further action taken by any other member of staff independently of these discussions and under no account should anyone else at school try to access the individuals account. The Area Manager will inform the relevant authorities with regards to the ICT equipment and make a decision about whether a strategy meeting to discuss the case needs to be held.

3.5 In order to assist with this process the Headteacher should ensure that: Equipment suspected of being involved with inappropriate use cannot be used by anyone, should be clearly identified, stored securely and only relevant authorities or the police be given access to carry out any investigation.

3.6 If a social web site is thought to contain defamatory or intimidating material, the site owners should be contacted and provided with details of the account and location of that material. Site owners will usually investigate and remove such material or deny access of the account holder to their service.

3.7 The school's Broadband Service Provider will ensure effective levels of security and internet filtering.

3.8 All third party ICT support staff should undergo a DBS check.

4 USER RESPONSIBILITIES

The following should be read in conjunction with the school's Online Safety Policy, and the Acceptable Use Agreement for Staff, Governors and Volunteers (see Appendix 1):

4.1 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.

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

4.3 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.

4.4 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 General Data Protection Regulations 2018. Care must also be taken not to breach another person's copyright, trademark or design, nor to publish any defamatory content.

4.5 Staff who have been given the use of a school laptop will be expected to sign for its use on receipt. Equipment taken off site must not be left unattended in a public place. This includes any items securely locked in the boot of a car, which invalidates the council's insurance. All reasonable care should be taken at all times by the custodian of the equipment, especially when travelling. Staff should be aware that if using equipment in a public place they may be overheard or documents read.

4.6 Staff may use school equipment for authorised business use only, except as allowed for in paragraph 5.1.

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

4.8 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.

4.9 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.

4.10 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.

4.11 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.

4.12 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.

4.13 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.

4.13 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.

4.14 Within the terms of the General Data Protection Regulations 2018, Human Rights Act 1998 and the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, the MAT 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 MAT 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.

4.15 Do not send private, sensitive or confidential information by unencrypted email – particularly to an external recipient - 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.

4.16 Websites should not be created on school equipment without the written permission of the Headteacher.

4.17 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.

4.18 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
- Send on chain mail or other materials that recipients, intended or otherwise, may regard as coercive or pressuring them into a course of action.
- Any other material that could have a negative impact on the safety and wellbeing of children and young people.
- This list is by no means exhaustive and other internet usage may also be considered inappropriate.

4.19 It is possible to access or be directed to inappropriate websites sites by accident, if this occurs staff should notify the headteacher as soon as possible.

4.20 Staff must use caution when posting information online including on social networking sites, blogs and text facilities. In particular staff are advised not to place any personal or confidential information on social websites as such information may be accessed by strangers. This could include other staff/pupils who might use the information in unintended, “unexpected” or possible “unpleasant” ways. Staff must not place any details relating to their professional life on any personal or social websites.

4.21 Staff must not post material damaging the reputation of the school or which could cause concern about their suitability to work with children or which breaches confidentiality. Staff posting material which could be considered inappropriate, could render themselves vulnerable to criticism or allegations of misconduct. Staff should bear in mind 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. If colleagues become aware of inappropriate material they should notify the Headteacher as soon as possible, providing a link to the web page. Under no circumstances should the content be forwarded.

4.22 Inappropriate social use of the internet outside the workplace could result in disciplinary action, if it brings the school's reputation into disrepute or exposes it to potential liabilities.

4.23 Staff must not be 'friends' to, or communicate with, students on 'Facebook' and other social network or similar sites. If any pupil makes contact with staff as per the above, they must decline the request and notify the Headteacher or Online Safety Lead as soon as possible. The Headteacher or Online Safety Lead can then deal with the situation as appropriate.

4.24 Photographs of pupils must not be placed on personal social networking sites or the school's website without parental or guardian consent. This is personal related data and individuals must be aware that this information is being published. Failure to obtain consent could result in formal action being taken

5 PERSONAL USE & PRIVACY

5.1 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.

5.2 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.

6 MOBILE PHONE COMMUNICATION AND INSTANT MESSAGING

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

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

6.3 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.

6.4 Staff should only communicate electronically with pupils from school accounts on approved school business, e.g. coursework.

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

6.6 Except in emergencies, mobile phones should not be used during contact time with the children e.g. texting. If mobile phone access is required during contact time, this must be discussed and agreed with the Headteacher

Appendix 1
Hartest CE Primary School
Acceptable Use Agreement for Staff, Governors and Visitors

This agreement applies to all online use and to anything that may be downloaded or printed.

All adults within the school/education setting or other establishment must be aware of their safeguarding responsibilities when using any online technologies, such as the internet, e-mail or social networking sites. They are asked to sign this Acceptable Use Agreement so that they provide an example to children and young people for the safe and responsible use of online technologies. This will educate, inform and protect adults so that they feel safeguarded from any potential allegations or inadvertent misuse themselves.

- I know that I must only use the school/education setting or other establishment equipment in an appropriate manner and for professional uses.
- I understand that I need to give permission to children and young people before they can upload images (video or photographs) to the internet or send them via e-mail.
- I know that images should not be inappropriate or reveal any personal information of children and young people if uploading to the internet.
- I have read the Procedures for Incidents of Misuse so that I can deal with any problems that may arise, effectively.
- I will report accidental misuse.
- I will report any incidents of concern for a child or young person's safety to the Headteacher, DSL / Online Safety Lead in accordance with procedures listed in the Acceptable Use Policy.
- I know who my DSL / Online Safety Lead is.
- I know that I am putting myself at risk of misinterpretation and allegation should I contact children and young people via personal technologies, including my personal e-mail. I know I should use the school/education setting or other establishment e-mail address and phones (if provided) and only to a child's school/education setting or other establishment e-mail address upon agreed use within the school/education setting or other establishment.
- I know that I must not use the school/education setting or other establishment system for personal use unless this has been agreed by the Headteacher or DSL / Online Safety Lead.
- I know that I should complete virus checks on my laptop and memory stick or other devices so that I do not inadvertently transfer viruses, especially where I have downloaded resources.
- I will ensure that I follow General Data Protection Regulations 2018 and have checked I know what this involves.
- I will ensure that I keep my password secure and not disclose any security information unless to appropriate personnel. If I feel someone inappropriate

requests my password I will check with the Online Safety Lead prior to sharing this information.

- I will adhere to copyright and intellectual property rights.
- I will only install hardware and software I have been given permission for.
- I accept that the use of any technology designed to avoid or bypass the school/education setting or other establishment filtering system is forbidden. I understand that intentional violation of this rule may result in disciplinary procedures being initiated.
- I have been given a copy of the Acceptable Use Policy to refer to about all e-safety issues and procedures that I should follow.

I have read, understood and agree with these Agreement as I know that by following them I have a better understanding of Online Safety and my responsibilities to safeguard children and young people when using online technologies.

Signed…………………………………………………Date…………………….

Name (printed)…………………………………………………