Hintlesham and Chattisham Church of England Primary School

St Edmundsbury and Ipswich Diocesan Multi Academy Trust

Staff Acceptable Use of ICT Policy

Signature of Headteacher	
Approved by **The Local Governing Body**	Hintlesham and Chattisham CE Primary
Signature of Chair of Governors	
Date approved	June 2020
Review date	June 2021

Staff Acceptable Use of ICT Policy

1. Introduction

2. This policy has been written in conjunction with the Policy for Child Acceptable Use of ICT and should be read in conjunction with other relevant school and County Council policies, procedures and Codes of Conduct including:

- Social Media Policy
- ICT Policy
- Disciplinary Procedure

3. Staff should be given sufficient training and knowledge to be able to recognise and report potential misuse and to enable them to use software and systems as relevant to their role. Staff are encouraged to make use of the resources developed by Childnet (http://www.childnet.com)

4. It is not the intention of the policy to try to police every social relationship that governors may have with parents and school staff but about reminding individuals of the importance of appropriate boundaries, including through their social media use.

1. Application

2. This policy applies to the school governing body, all teaching and other staff, whether employed by the St Edmundsbury and Ipswich Diocesan Multi-Academy Trust or employed directly by the school, external contractors providing services on behalf of the school the DMAT or the County Council, teacher trainees and other trainees, volunteers and other individuals who work for or provide services on behalf of the school. These individuals are collectively referred to in this policy as staff or staff members.

3. The policy applies in respect of all ICT resources and equipment within the school and resources that have been made available to staff for working at home. ICT resources and equipment includes computer resources, use of school internet access and email systems, software (including use of software such as SAP and SIMS), school telephones and text systems, cameras and recording equipment, intranet and virtual learning environment and any other electronic or communication equipment used in the course of the employee or volunteer's work. This policy also provides advice to staff in respect of the potential risks and consequences in relation to inappropriate use of their own personal ICT facilities, where this use is inconsistent with the expectations of staff working with children and young people.

1. Access

2. School staff will be provided with a log on where they are entitled to use the school ICT facilities and advised what hardware and software they are permitted to access, including access to the internet and email. Unless indicated, staff can use any facilities available subject to the facilities not being in use by pupils or other colleagues. Access is provided to enable staff to both perform their role and to enable the wider staff in the school to benefit from such facilities.

3. Where staff have been provided with a school email address to enable them to perform their role effectively, it will not normally be used to communicate with parents and pupils. Where staff are able to access email outside of school's hours, the email facility should not routinely be used to email parents outside of normal school hours.

4. Access to certain software packages and systems (e.g.PS Financials, iTrent, SIMS, RAISE Online, FFT, Target Tracker, school texting services, remote access) will be restricted to nominated staff and unless permission and access has been provided, staff must not access these systems.

5. Some staff may be provided with laptops and other equipment for the performance of their role. Where provided, staff must ensure that their school laptop/other equipment is password protected and not accessible by others when in use at home and that it is not used inappropriately by themselves or others. Staff must also ensure that they bring their laptop/equipment in as required for updating of software, licenses and virus protection.

6. Where the school provides digital cameras and other recording equipment for educational and school business use and it is used away from the school site, it must be kept secure and safe. Where pictures of pupils are taken, staff must ensure that they ensure consent has been provided by parents, and that the school's policy in relation to use of pictures, is followed.

7. If the school does not provide school mobile phones, staff may use, in urgent or emergency situations during off site visits, their personal mobile telephones. Where used in these emergency situations and a cost incurred, the school will provide reimbursement of the cost of any calls made. Should staff need to make contact whilst off site, this should normally be undertaken via the school rather than a direct call from the individual's personal mobile. If not staff should withhold their number. School staff who have access to colleagues' personal contact details must ensure that they are kept confidential.

8. No mobile telephones or similar devices, even those with hands free facilities should be used whilst driving on school business.

9. School staff have access to the school telephone system for personal use in an emergency, but permission must be asked from the Headteacher. Where such use is made of this facility, it must be done during break periods, must not be excessive and the school should require either the cost of the call or a donation to be made towards the cost of the call.

10. The school will ensure that Display Screen Equipment assessments are undertaken in accordance with its Health and Safety Policy.

1. Communication with parents, pupils and governors

2. The school communicates with parents and governors through a variety of mechanisms. The points below highlight who is normally authorised to use which systems and can directly communicate without requiring any approval before use or to agree content. School must indicate to staff if any other staff are permitted to make contact using the systems below:

2.1. School Telephones – all teachers, administrative staff and staff who have been permitted through their roles in pupil welfare or home/school link staff. Normally teaching assistants and lunchtime supervisory staff would need to seek approval from a class teacher where they feel they need to make a telephone call to a parent.

2.2. Text System – Office staff. Where, in exceptional circumstances other staff need to send a text, this is normally approved by a member of the Senior Leadership Team.

2.3. Letters – Normally all teachers may send letters home, but they may be required to have these approved by the Headteacher before sending. Where office staff send letters home these will normally require approval by the Headteacher.

2.4. Email – school email accounts should not routinely be used for communication with parents outside school hours. Email is used as a normal method of communication amongst school governors and where governors are linked in particular areas with members of staff, communication may take place via email.

3. Under normal circumstances, school staff should not be using any of the methods outlined above to communicate directly with pupils. If a member of staff needs to contact a pupil direct via any of these methods, this must be approved by the Headteacher.

4. Where pupils are submitting work electronically to school staff, this must be undertaken using school systems and not via personal email.

1. Social Media

2. School staff are advised to exercise extreme care in their personal use of social networking sites, giving consideration to their professional role working with children. Staff should make appropriate use of the security settings available through social networking sites and ensure that they keep them updated as the sites change their settings. Staff are advised that inappropriate communications that come to the attention of the school can lead to disciplinary action, including dismissal.

3. Expectations of staff when using social media.

1. Unacceptable Use

2. Appendix 1 provides a list of Do's and Dont's for school staff to enable them to protect themselves from inappropriate use of ICT resources and equipment. School systems and resources must not be used under any circumstances for the following purposes:

2.1. to communicate any information that is confidential to the school or to communicate/share confidential information which the member of staff does not have authority to share

2.2. to present any personal views and opinions as the views of the school, or to make any comments that are libelous, slanderous, false or misrepresent others

2.3. to access, view, download, post, email or otherwise transmit pornography, sexually suggestive or any other type of offensive, obscene or discriminatory material

2.4. to communicate anything via ICT resources and systems or post that may be regarded as defamatory, derogatory, discriminatory, harassing, bullying or offensive, either internally or externally

2.5. to communicate anything via ICT resources and systems or post that may be regarded as critical of the school, the leadership of the school, the school's staff or its pupils

2.6. to upload, download, post, email or otherwise transmit or store material that contains software viruses or any other computer code, files or programmes designed to interrupt, damage, destroy or limit the functionality of any computer software or hardware or telecommunications equipment

2.7. to collect or store personal information about others without direct reference to The Data Protection Act

2.8. to use the school's facilities to undertake any trading, gambling, other action for personal financial gain, or political purposes, unless as part of an authorised curriculum project

2.9. to use the school's facilities to visit or use any online messaging service, social networking site, chat site, web-based email or discussion forum not supplied or authorised by the school

2.10. to undertake any activity (whether communicating, accessing, viewing, sharing. uploading or downloading) which has negative implications for the safeguarding of children and young people.

2. Any of the above activities are likely to be regarded as gross misconduct, which may, after proper investigation, lead to dismissal. If employees are unsure about the use of ICT resources including email and the intranet, advice should be sought from a member of the Senior Leadership Team or ICT lead if applicable.

3. Where an individual accidentally accesses a website or material that they consider to be pornographic or

offensive, this should be reported immediately to the Headteacher or other member of the senior leadership team. Schools are encouraged to use appropriate blocking software to avoid the potential for this to happen. Reporting to the Headteacher or senior leadership team equally applies where school staff are using school equipment or facilities at home and accidentally access inappropriate sites or material. Genuine mistakes and accidents will not be treated as a breach of this policy.

4. Where an individual has been communicated with in a manner outlined above (e.g. has received an inappropriate email or attachment), they are advised to report this immediately to the Headteacher or another member of the senior leadership team so that this can be dealt with appropriately.

1. Personal and private use

2. All school staff with access to computer equipment, including email and internet, are permitted to use them for occasional personal use provided that this is access is not:

2.1. taking place at the expense of contracted working hours (i.e. is not taking place during paid working time)

2.2. interfering with the individual's work

2.3. relating to a personal business interest

2.4. involving the use of news groups, chat lines or similar social networking services

2.5. at a cost to the school

2.6. detrimental to the education or welfare of pupils at the school

3. Excessive personal use of school facilities is likely to be considered to be a disciplinary matter, may lead to restricted access to computer equipment and where costs are incurred (e.g. personal telephone use), the school will seek reimbursement from the member of staff.

4. It is important for staff to also be aware that inappropriate use of their own personal or other ICT facilities in their personal time, can have implications for their employment situation where this becomes known and the activities that are undertaken are inconsistent with the expectations of staff working with children and young people.

5. Where school staff have brought their own personal equipment such as mobile telephones, digital assistants, laptops and cameras, into the school, these personal items, should not be used during pupil contact sessions unless authorised. Staff should follow all points outlined in this section in relation to their personal use. Staff should ensure that there is no inappropriate content on any of these pieces of equipment and ensure that they are not accessed by pupils at any time. Such equipment should not normally be required to enable staff to undertake their role but where it is used, staff should take care to ensure any school data/images are deleted following authorised use of the equipment.

6. Whilst individuals may be required to use their personal mobile telephone to make contact with the school, staff should exercise care and seek reimbursement as outlined in section 3.

1. Security and confidentiality

2. Any concerns about the security of the ICT system should be raised with a member of the senior leadership team

3. Staff are required to ensure that they keep any passwords confidential, do not select a password that is easily guessed and regularly change such passwords.

4. School staff must take account of any advice issued regarding what is permitted in terms of downloading educational and professional material to the school server. Where staff are provided with a password protected memory stick for such activity, to both protect the integrity of the server and to save space, this should be used. All staff must review the appropriateness of the material that they are downloading prior to downloading and are encouraged to do so from known and reputable sites to protect the integrity of the school's systems. Where problems are encountered in downloading material, this should be reported to the school's ICT lead.

5. Where staff are permitted to work on material at home and bring it in to upload to the school server through their password protected memory sticks, they must ensure that they have undertaken appropriate virus checking on their systems. Where provided, staff should normally use their school issued laptop for such work.

6. Staff must ensure that they follow appropriate and agreed approval processes before uploading material for use by pupils to the pupil ICT system.

7. Whilst any members of school staff may be involved in drafting material for the school website, staff must ensure that they follow appropriate and agreed approval processes before uploading material to the website.

8. The school will nominate staff who are responsible for ensuring that all equipment is regularly updated with new software including virus packages and that licenses are maintained on all school based and school issued equipment. Staff must ensure that they notify the nominated staff when reporting any concerns regarding potential viruses, inappropriate software or licenses.

9. Staff must ensure that their use of the school's ICT facilities does not compromise rights of any individuals under the Data Protection Act. This is particularly important when using data off site and electronic data must only be

taken off site in a secure manner, either through password protection on memory pens or through encrypted memory pens. This is also particularly important when communicating personal data via email rather than through secure systems. In these circumstances, staff must ensure that they have the correct email address and have verified the identity of the person that they are communicating the data with.

10. Staff must also ensure that they do not compromise any rights of individuals and companies under the laws of Copyright through their use of ICT facilities.

1. Monitoring

2. The school is part of the DMAT and therefore is required to comply with their email, internet and intranet policies.

3. The school and DMAT reserve the right to monitor the use of email, internet and intranet communications and where necessary data may be accessed or intercepted in the following circumstances:

3.1. To ensure that the security of the school and county council's hardware, software, networks and systems are not compromised

3.2. To prevent or detect crime or unauthorised use of the school or county council's hardware, software, networks or systems

3.3. To gain access to communications where necessary where a user is absent from work

4. Where staff have access to the internet during the course of their work, it is important for them to be aware that the school or county council may track the history of the internet sites that have been visited.

5. To protect the right to privacy, any interception of personal and private communications will not take place unless grounds exist to show evidence of crime, or other unlawful or unauthorised use. Such interception and access will only take place following approval by the Chair of Governors, after discussions with relevant staff in St Edmundsbury and Ipswich DMAT HR, IT and Audit Services and following an assessment to determine whether access or interception is justified.

1. Whistleblowing and cyberbullying

2. Staff who have concerns about any abuse or inappropriate use of ICT resources, virtual learning environments, camera/recording equipment, telephony, social networking sites, email or internet facilities or inappropriate communications, whether by pupils or colleagues, should alert the Headteacher to such abuse. Where a concern relates to the Headteacher, this should be disclosed to the Chair of Governors. If any matter concerns child safety, it should also be reported to the Designated Safeguarding Lead (DSL).

3. It is recognised that increased use of ICT has led to cyberbullying and/or concerns regarding e-safety of school staff. Staff are strongly advised to notify their Headteacher where they are subject to such circumstances. Advice can also be sought from professional associations and trade unions. Support is also available through the Schools Choice confidential counselling service, Employee Support Line (08001164368) and also via the UK Safer Internet Centre helpline@safetinternet.otg.uk or 0844 381 4772

1. Remote Access Policy

Hintlesham and Chattisham Primary School provides remote access to help support employees with the delivery of the curriculum and for teaching and learning. It is also intended for managing and administering the ICT networks. Use of the school's remote access service implies acceptance of the conditions of use. The school may refuse to extend remote access privileges to any employee or terminate a remote access arrangement at any time.

1. Uses of Remote Access Services

The following list is not exhaustive, but sets out broad areas which the school considers to be acceptable use of remote access.

- To gain access to School Information Management System (SIMS)
- To gain access to resources, files and software on the school network
- To administer the school network remotely

2. Use of Computers and Equipment

Any computer used to access the school's remote systems must possess anti-virus and anti-spyware programs. These must be updated regularly, at least once a week. The school bears no responsibility if use of the remote access system causes system crashes, or complete or partial data loss on connected computers. Users of remote access are solely responsible for backing up all data before accessing the system. At its discretion, the school will disallow remote access for any computer that proves incapable, for any reason, of working correctly with the remote access system.

3. Potential Security Issues

1. Viruses and malware:

When a computer is directly connected to the internet it can be contacted by any other computer also connected to the internet. As a result, there is a risk of exposure to malware that could connect to and potentially compromise that computer, which in turn risks infecting the school's system. For this reason, precautions must be taken to minimise this risk:

- Make sure up-to-date anti-virus software is installed.

- Make sure the latest operating system patches are installed.
- Run a weekly virus scan.
- If a computer has become infected with a virus or other malware, do not use it to remotely access the school's network until the virus has been deleted.
- Turn on phishing filters on web browsers to reduce the risk of phishing attacks.
- Use an anti-spyware program to detect spyware.

2. Data security:
To avoid a risk of confidential information being disclosed to unauthorised third parties:
   - Logout of remote access before leaving the computer.
   - Wireless network connections must be encrypted using WPA2 or use a cable connection.
   - Do not allow any unauthorised person, including family and friends, to use the remote access login or to access files held on the school's network.
   - Use a password protected screensaver to prevent anyone gaining access to the computer
   - Do not use password storing facilities found in some programs to automatically remember passwords.
   - Do not reveal passwords. If for any reason a password is revealed this should be changed

immediately. This policy will ensure that staff are able to access the school network remotely without risk to the security of the system.

1. **Signature**
2. It will be normal practice for staff to read and sign a declaration as outlined in Appendix 2, to confirm that they have had access to the acceptable use policy and that they accept and will follow its terms.
3. Staff must comply with the terms of this policy. Any breach will be considered to be a breach of disciplinary rules, which may lead to a disciplinary sanction (e.g. warning), dismissal, and/or withdrawal of access to ICT facilities. Staff should be aware, that in certain instances, inappropriate use of ICT may become a matter for police or social care investigations.