St Edmundsbury and Ipswich
Diocesan Multi Academy Trust

Long Melford CE Primary School

Acceptable Use of ICT and Mobile Phones Policy

Prepared By	*Amanda Woolmer - Headteacher*
Approved by the Committee/Governing body	*LGB – Long Melford CE Primary School*
Signature of Chair of Governors	*Cheryl Morgan*
Date Approved Updated	*January 2022* *January 2023*
Review Date	*January 2024*

Acceptable Use of ICT and Mobile Phones Policy

1.0 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.

This policy should be read in conjunction with other relevant school and Diocese of St Edmundsbury and Ipswich Multi-Academy Trust policies, procedures and Codes of Conduct including:

- Social Media and Phone Policy
- ICT Policy
- Online Safety Policy
- Disciplinary Procedure
- Child Protection and Safeguarding Policy

1.2 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.

1.3 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.

2.0 Application

2.1 This policy applies to the school governing body, all teaching and other staff, whether employed by the County Council or employed directly by the school, external contractors providing services on behalf of the school or Suffolk 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.

2.2 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 SIMS), school telephones and text systems, cameras and recording equipment, intranet 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.

3.0 Access

3.1 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.

3.2 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 schools hours, the email facility should not routinely be used to email parents outside of normal school hours.

3.3 Access to certain software packages and systems will be restricted to nominated staff and unless permission and access has been provided, staff must not access these systems.

3.4 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, licences and virus protection.

3.5 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.

3.6 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. School staff who have access to colleagues' personal contact details must ensure that they are kept confidential.

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

3.8 Whether school staff have access to the school telephone system for personal use will be confirmed by the school. 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.

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

4.0 Communication with parents, pupils and governors

4.1 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:

4.1.1 School Telephones – all teachers, administrative staff and staff who have been permitted through their roles in pupil welfare or home/school link staff.

4.1.2 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.

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

4.1.4 Email – This is used as a normal method of communication to parents, amongst school governors and where governors are linked in particular areas with members of staff, communication may take place via email.

4.2 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 Executive Headteacher.

4.3 Where pupils are submitting work electronically to school staff, this must be undertaken using the Office email account or the class accounts that have been set up to use in the event of Home Schooling.

5.0 Social Media

5.1 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.

5.2 Staff should refer to the School Social Media Policy which contains detailed advice on the expectations of staff when using social media.

6.0 Unacceptable Use

6.1 Appendix 1 provides a list of Do's and Don'ts 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:

6.1.1 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

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

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

6.1.4 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

6.1.5 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

6.1.6 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

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

6.1.8 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

6.1.9 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

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

6.2 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.

6.3 Where an individual accidently accesses a website or material that they consider to be pornographic or offensive, this should be reported immediately to the Executive Headteacher or the Head of School. Schools use appropriate filtering 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.

6.4 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.

7.0 Personal and private use

7.1 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:

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

7.1.2 interfering with the individual's work

7.1.3 relating to a personal business interest

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

7.1.5 at a cost to the school

7.1.6 detrimental to the education or welfare of pupils at the school

7.2 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.

7.3 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.

7.4 Where school staff have brought their own personal equipment such as mobile telephones, tablets, 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 use of the equipment.

7.5 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.

8.0 Security and confidentiality

8.1 Any concerns about the security of the ICT system should be raised with the Executive Headteacher or the Head of School.

8.2 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.

8.3 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. 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.

8.4 Staff must ensure that they follow appropriate and agreed approval processes before uploading material for use by pupils to the 'Class Pages' on the school's website.

8.5 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.

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

8.7 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 sticks or through encrypted memory sticks. 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.

8.8 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.

9.0 Monitoring

9.1 The school and St Edmundsbury and Ipswich Multi-Academy Trust 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:

9.1.1 to ensure that the security of the school's hardware, software, networks and systems are not compromised

9.1.2 to prevent or detect crime or unauthorised use of the school's hardware, software, networks or systems

9.1.3 to gain access to communications where necessary where a user is absent from work

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

9.3 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 Multi-Academy Trust, Suffolk County Council's HR, IT and Audit Services, LADO and following an assessment to determine whether access or interception is justified.

10.0 Whistleblowing and cyberbullying

10.1 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).

10.2 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.

10.3 Further advice on cyberbullying and harassment can be found in the School Social Media Policy and in the 'Cyber bullying: Practical Advice for School Staff' section of the ICT Policy.

11.0 Remote Access Policy – Long Melford Church of England Primary School provides remote access 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.

11.1 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 administer the school network remotely

11.2 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 month. 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.

11.3 Potential Security Issues

11.3.1 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.

11.3.2 Data security: To avoid a risk of confidential information being disclosed to unauthorised third parties:

• Logout of remote access before leaving any workstation/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.

12.0 Signature

12.1 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.

12.2 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.

Do's and Don'ts: Advice for Staff Appendix 1

Whilst the wide range of ICT systems and resources available to staff, both in school and outside of school, have irrefutable advantages, there are also potential risks that staff must be aware of. Ultimately if staff use ICT resources inappropriately, this may become a matter for a police or social care investigation and/or a disciplinary issue which could lead to their dismissal. Staff should also be aware that this extends to inappropriate use of ICT outside of school.

This Dos and Don'ts list has been written as a guidance document. Whilst it is not fully comprehensive of every circumstance that may arise, it indicates the types of behaviours and actions that staff should not display or undertake as well as those that they should in order to protect themselves from risk.

General issues

Do	**Don't**
• ensure that you do not breach any restrictions that there may be on your use of school resources, systems or resources • ensure that where a password is required for access to a system, that it is not inappropriately disclosed • respect copyright and intellectual property rights • ensure that you have approval for any personal use of the school's ICT resources and facilities • be aware that the school's systems will be monitored and recorded to ensure policy compliance • ensure you comply with the requirements of the Data Protection Act when using personal data • seek approval before taking personal data off of the school site • ensure personal data is stored safely and securely whether kept on site, taken off site or accessed remotely • report any suspected misuse or concerns that you have regarding the school's systems, resources and equipment to the Executive Headteacher or designated manager and/or Designated Safeguarding Lead (DSL) as appropriate • be aware that a breach of your school's Acceptable Use Policy will be a disciplinary matter and in some cases, may lead to dismissal • ensure that any equipment provided for use at home is not accessed by anyone not approved to use it	• access or use any systems, resources or equipment without being sure that you have permission to do so • access or use any systems or resources or equipment for any purpose that you don't have permission to use the system, resources or equipment for • compromise any confidentiality requirements in relation to material and resources accessed through ICT systems • use systems, resources or equipment for personal use without having approval to do so • use other people's log on and password details to access school systems and resources • download, upload or install any hardware or software without approval • use unsecure removable storage devices to store personal data • use school systems for personal financial gain, gambling, political activity or advertising • communicate with parents and pupils outside normal working hours unless absolutely necessary

• ensure that you have received adequate training in ICT • ensure that your use of ICT bears due regard to your personal health and safety and that of others	

Use of telephones, mobile telephones and instant messaging

Do	**Don't**
• ensure that your communications are compatible with your professional role • ensure that you comply with the school's policy on use of personal mobile telephones • ensure that you reimburse the school for personal telephone calls as required • keep personal phones locked away during school hours	• send messages that could be misinterpreted or misunderstood • excessively use the school's telephone system for personal calls • use personal or school mobile telephones when driving or around children • use the camera function on personal mobile telephones unless you have specific permission from the Headteacher to take images of colleagues, pupils or of the school

Use of cameras and recording equipment

Do	**Don't**
• ensure that material recorded is for educational purposes only, using school equipment • ensure that where recording equipment is to be used, approval has been given to do so • ensure that material recorded is stored appropriately and destroyed in accordance with the school's policy • ensure that parental consent has been given before you take pictures of school pupils (See GDPR feedback forms)	• bring personal recording equipment into school without the prior approval of the Headteacher • inappropriately access, view, share or use material recorded other than for the purposes for which it has been recorded

Use of email and the internet

Do	**Don't**
• alert your Headteacher or designated manager if you receive inappropriate content via email	• use personal email addresses to communicate with pupils or parents

• be aware that the school's email system will be monitored and recorded to ensure policy compliance • ensure that your email communications are compatible with your professional role • give full consideration as to whether it is appropriate to communicate with pupils or parents via email, or whether another communication mechanism (which may be more secure and where messages are less open to misinterpretation) is more appropriate • be aware that the school may intercept emails where it believes that there is inappropriate use • seek support to block spam • alert your Headteacher or designated manager if you accidentally access a website with inappropriate content • be aware that a website log is recorded by the school and will be monitored to ensure policy compliance • answer email messages from pupils and parents within your directed time • mark personal emails by typing 'Personal/Private' within the subject header line • Ensure that you are the only person who has access to your personal email address when using it for school communication (Governors only)	• send messages in the heat of the moment • send messages that may be construed as defamatory, discriminatory, derogatory, offensive or rude • use email systems to communicate with parents or pupils unless approved to do so • download attachments from emails without being sure of the security and content of the attachment • forward email messages without the sender's consent unless the matter relates to a safeguarding concern or other serious matter which must be brought to a senior manager's attention • access or download inappropriate content (material which is illegal, obscene, libellous, offensive or threatening) from the internet • upload any material onto the school website that doesn't meet style requirements and without approval

Use of social networking sites

Do	**Don't**
• ensure that you understand how any site you use operates and therefore the risks associated with using the site • familiarise yourself with the processes for reporting misuse of the site • consider carefully who you accept as friends on a social networking site • exercise caution when accepting friendship requests from parents - – you may be giving them access to	• access social media webpages using school equipment • accept friendship requests from pupils • put information or images on line or share them with colleagues, pupils, or parents (either on or off site) when the nature of the material may be controversial • post anything that may be interpreted as slanderous towards colleagues, pupils or parents • use social networking sites to contact parents and/or pupils

personal information, and allowing them to contact you inappropriately • report to your Headteacher any incidents where a pupil has sought to become your friend through a social networking site • take care when publishing information about yourself and images of yourself on line – assume that anything you release will end up in the public domain • ask yourself about whether you would feel comfortable about a current or prospective employer, colleague, pupil or parent viewing the content of your page • follow school procedures for contacting parents and/or pupils	

The development of new technologies and systems e.g. mobile phones, email and social networking websites means that bullying is often now taking on a new form; online-bullying. Victims of online bullying can experience pain and anxiety as much as traditional forms of bullying, particularly as it can occur outside of the school and school hours, significantly intruding into the personal life of the victim. Whilst it is difficult for schools and teachers to deal with this as they have no direct control over external websites there are a range of actions that school staff can take to reduce the chances of online-bullying occurring and actions that can be undertaken where it has already occurred.

The guidelines for Headteachers and Governors in dealing with allegations of bullying or harassment define online bullying as "the use of information and communication technologies to threaten, harass, humiliate, defame or impersonate". Online bullying may involve email, virtual learning environments, chat room, social networking sites, mobile and landline telephones, digital camera images and game and virtual world sites. This practical advice supplements the guidelines and provides links to other guidance available to school staff in relation to Online - bullying.

By signing below, you agree to the terms and conditions outlined above:

Name:_____

Signed:_____

Date:_____

Acceptable Use Policy

Please sign this sheet and return to Louise Gamble. It will be placed on your School Personnel File.

By signing below, you agree to the terms and conditions outlined above:

Name:_____

Signed:_____

Date:_____