Moreton Church of England Primary School

e-Safety and Internet Use Policy

Written by: N Batt, Headteacher

Date: September 2020

(updated 2022)

Agreed by Governors (Date):

Signed (CoG):

Moreton Church of England Primary School

'Growing Together in Faith, Knowledge and Love'

Contents

Moreton Church of England Primary School

1. Introduction and Overview

Rationale

The purpose of this policy is to:

- Set out the key principles expected of all members of the school community at Moreton Church of England Primary School with respect to the use of IT-based technologies.
- Safeguard and protect the children and staff.
- Assist school staff working with children to work safely and responsibly with the Internet and other IT and communication technologies and to monitor their own standards and practice.
- Set clear expectations of behaviour and/or codes of practice relevant to responsible use of the Internet for educational, personal or recreational use for the whole school community.
- Have clear structures to deal with online abuse such as online bullying [noting that these need to be cross referenced with other school policies].
- Ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- Minimise the risk of misplaced or malicious allegations made against adults who work with students.

The main areas of risk for our school community can be summarised as follows:

Content

- Exposure to inappropriate content
- Lifestyle websites promoting harmful behaviours
- Hate content
- Content validation: how to check authenticity and accuracy of online content

Contact

- Grooming (sexual exploitation, radicalisation etc.)
- Online bullying in all forms
- Social or commercial identity theft, including passwords

Conduct

- Aggressive behaviours (bullying)
- Privacy issues, including disclosure of personal information
- Digital footprint and online reputation
- Health and well-being (amount of time spent online, gambling, body image)

- Sexting
- Copyright (little care or consideration for intellectual property and ownership)

Scope

This policy applies to all members of Moreton Church of England Primary School community (including staff, students/pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of school and/or academy IT systems, both in and out of school.

Roles and responsibilities

Role	Key Responsibilities
Headteacher and DSL: **Mrs Batt** Deputy Headteacher: **Miss French** Deputy DSLs: **Mrs R Barros** **Mrs A Mead**	• Must be adequately trained in off-line and online safeguarding, in-line with statutory guidance and relevant Local Safeguarding Children Board (LSCB) guidance • To lead a 'safeguarding' culture, ensuring that online safety is fully integrated with whole school safeguarding. • To take overall responsibility for online safety provision • To take overall responsibility for data management and information security (SIRO) ensuring school's provision follows best practice in information handling • To ensure the school uses appropriate IT systems and services including, filtered Internet Service, e.g. United Networks • To be responsible for ensuring that all staff receive suitable training to carry out their safeguarding and online safety roles • To be aware of procedures to be followed in the event of a serious online safety incident • Ensure suitable 'risk assessments' undertaken so the curriculum meets needs of pupils, including risk of children being radicalised • To receive regular monitoring reports from the Online Safety/Computing Subject Lead • To ensure that there is a system in place to monitor and support staff who carry out internal online safety procedures, e.g. network manager • To ensure Governors are regularly updated on the nature and effectiveness of the school's arrangements for online safety • To ensure school website includes relevant information.

Moreton Church of England Primary School

Role	Key Responsibilities
Online Safety Officer: **Mrs Batt** **Mrs Brumby as adviser/support** Designated Child Protection Lead: **Mrs Batt**	• Take day to day responsibility for online safety issues and a leading role in establishing and reviewing the school's online safety policy/documents • Promote an awareness and commitment to online safety throughout the school community • Ensure that online safety education is embedded within the curriculum • Liaise with school technical staff where appropriate • To communicate regularly with SLT and the designated online safety Governor/committee to discuss current issues, review incident logs and filtering/change control logs • To ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident • To ensure that online safety incidents are logged as a safeguarding incident, where appropriate • Facilitate training and advice for all staff • Oversee any pupil surveys / pupil feedback on online safety issues • Liaise with the Local Authority and relevant agencies • Is regularly updated in online safety issues and legislation, and be aware of the potential for serious child protection concerns.
Governors/Safeguarding governor (including online safety) **Mrs L Godfrey**	• To ensure that the school has in place policies and practices to keep the children and staff safe online • To approve the Online Safety Policy and review the effectiveness of the policy • To support the school in encouraging parents and the wider community to become engaged in online safety activities • The role of the online safety Governor will include: regular review with the online safety Co-ordinator.
Computing Curriculum Leader: **Mrs Brumby**	• To oversee the delivery of the online safety element of the Computing curriculum
Network Manager/technician: **United Net**	• To report online safety related issues that come to their attention, to the Online Safety Coordinator • To manage the school's computer systems, ensuring - school password policy is strictly adhered to. - systems are in place for misuse detection and malicious attack (e.g. keeping virus protection up to date) - access controls/encryption exist to protect personal and sensitive

Role	Key Responsibilities
	information held on school-owned devices - the school's policy on web filtering is applied and updated on a regular basis • That they keep up to date with the school's online safety policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant • That the use of school technology and online platforms are regularly monitored and that any misuse/attempted misuse is reported to the online safety co-ordinator/Headteacher • To ensure appropriate backup procedures and disaster recovery plans are in place • To keep up-to-date documentation of the school's online security and technical procedures
Data and Information (Asset Owners) Managers (IAOs): **Mrs Mainwaring** **Steve Roberts from 1159 Productions**	• To ensure that the data they manage is accurate and up-to-date • Ensure best practice in information management. i.e. have appropriate access controls in place, that data is used, transferred and deleted in-line with data protection requirements. • The school must be registered with Information Commissioner
Teachers: **See website for list of current staff**	• To embed online safety in the curriculum • To supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant) • To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws
All staff, volunteers and contractors: **See website for list of current staff**	• To read, understand, sign and adhere to the school staff Acceptable Use Agreement, and understand any updates annually. The AUP is signed by new staff on induction. • To report any suspected misuse or problem to the online safety coordinator • To maintain an awareness of current online safety issues and guidance e.g. through CPD • To model safe, responsible and professional behaviours in their own use of technology **Exit strategy** • At the end of the period of employment/volunteering to return any

Role	Key Responsibilities
	equipment or devices loaned by the school. This will include leaving PIN numbers, IDs and passwords to allow devices to be reset, or meeting with line manager and technician on the last day to log in and allow a factory reset.
Pupils	• Read, understand, sign and adhere to the Pupil Acceptable Use Agreement annually – to be implemented in September 2020. • To understand the importance of reporting abuse, misuse or access to inappropriate materials • To know what action to take if they or someone they know feels worried or vulnerable when using online technology • To understand the importance of adopting safe behaviours and good online safety practice when using digital technologies out of school and realise that the school's online safety policy covers their actions out of school • To contribute to any 'pupil voice' / surveys that gathers information of their online experiences
Parents/carers	• To read, understand and promote the school's Pupil Acceptable Use Agreement with their child/ren - to be implemented in September 2020 • to consult with the school if they have any concerns about their children's use of technology • to support the school in promoting online safety and endorse the Parents' Acceptable Use Agreement which includes the pupils' use of the Internet and the school's use of photographic and video images
External groups including Parent groups	• Any external individual/organisation will sign an Acceptable Use agreement prior to using technology or the Internet within school • to support the school in promoting online safety • To model safe, responsible and positive behaviours in their own use of technology.

Communication:

The policy will be communicated to staff/pupils/community in the following ways:

- Policy to be posted on the school website/ policy folder in the office.
- Policy to be discussed as part of school induction pack for new staff.
- Regular updates and training on online safety for all staff.
- Acceptable use agreements discussed with staff and pupils at the start of each year. Acceptable use agreements to be issued to whole school community, on entry to the school.

Handling Incidents:

- The school will take all reasonable precautions to ensure online safety.
- Staff and pupils are given information about infringements in use and possible sanctions.
- The Online Officer acts as the first point of contact for any incident. This is supported by the Network manager.
- Any suspected online risk or infringement is reported to Online Safety Coordinator that day
- Any concern about staff misuse is always referred directly to the Headteacher, unless the concern is about the Headteacher in which case the compliant is referred to the Chair of Governors and the LADO (Local Authority's Designated Officer).

Review and Monitoring

The online safety policy is referenced within other school policies (e.g. Safeguarding and Child Protection policy, Anti-Bullying policy, PSHE, Computing policy).

- The online safety policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the school
- There is widespread ownership of the policy and it has been agreed by the SLT and accepted by the Local Governing Body. All amendments to the school online safety policy will be disseminated to all members of staff and pupils.

2. Education and Curriculum

Pupil online safety curriculum

This school:

- has a clear, progressive online safety education programme as part of the Computing curriculum/PSHE and other curriculum areas as relevant. This covers a range of skills and behaviours appropriate to their age and experience;
- plans online use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas;
- will remind students about their responsibilities through the pupil Acceptable Use Agreement(s);
- ensures staff are aware of their responsibility to model safe and responsible behaviour in their own use of technology, e.g. use of passwords, logging-off, use of content, research skills, copyright;
- ensures that staff and pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright/intellectual property rights;
- ensure pupils only use school-approved systems and publish within appropriately secure / age-appropriate environments.

Staff and governor training

This school:

- makes regular training available to staff on online safety issues and the school's online safety education program;
- provides, as part of the induction process, all new staff [including those on university/college placement and work experience] with information and guidance on the Online Safety Policy and the school's Acceptable Use Agreements.

Parent awareness and training

This school:

- provides induction for parents with training sessions and as part of our transition information evening which includes online safety;
- runs a rolling programme of online safety advice, guidance and training for parents.

3. Expected Conduct and Incident management

Expected conduct

In this school, all users:

- are responsible for using the school IT and communication systems in accordance with the relevant Acceptable Use Agreements;
- understand the significance of misuse or access to inappropriate materials and are aware of the consequences;
- understand it is essential to reporting abuse, misuse or access to inappropriate materials and know how to do so;
- understand the importance of adopting good online safety practice when using digital technologies in and out of school;
- know and understand school policies on the use of mobile and hand held devices including cameras;

Staff, volunteers and contractors

- know to be vigilant in the supervision of children at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas where older pupils have more flexible access;
- know to take professional, reasonable precautions when working with pupils, previewing websites before use; using age-appropriate (pupil friendly) search engines where more open Internet searching is required with younger pupils;

Parents/Carers

- should provide consent for pupils to use the Internet, as well as other technologies, as part of the online safety acceptable use agreement form;
- should know and understand what the school's 'rules of appropriate use for the whole school community' are and what sanctions result from misuse.

Incident Management

In this school:

- there is strict monitoring and application of the online safety policy and a differentiated and appropriate range of sanctions;
- all members of the school are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the school's escalation processes;
- support is actively sought from other agencies as needed (i.e. the local authority, UK Safer Internet Centre helpline, CEOP, Prevent Officer, Police, IWF) in dealing with online safety issues;
- monitoring and reporting of online safety incidents takes place and contribute to developments in policy and practice in online safety within the school;
- parents/carers are specifically informed of online safety incidents involving young people for whom they are responsible;
- the Police will be contacted if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law;
- we will immediately refer any suspected illegal material to the appropriate authorities – Police, Internet Watch Foundation and inform the LA.

4. Managing IT and Communication System

Internet access, security (virus protection) and filtering

This school:

- informs all users that Internet/email use is monitored;
- has the educational filtered secure broadband connectivity through United Network;
- uses a filtering system which blocks sites that fall into categories (e.g. adult content, race hate, gaming). All changes to the filtering policy are logged and only available to staff with the approved 'web filtering management' status;
- ensures network health through use of anti-virus software;
- Uses DfE, LA or approved systems to send 'protect-level' (sensitive personal) data over the Internet

Network management (user access, backup)

This school

- Uses individual, audited log-ins for all user;
- Uses guest accounts occasionally for external or short term visitors for temporary access to appropriate services;
- Has additional local network monitoring systems in place;
- Ensures the Systems Administrator/network manager is up-to-date with relevant services and policies;
- Has daily back-up of school data (admin and curriculum);
- Uses secure, 'Cloud' storage for data back-up that conforms to DfE guidance;
- Storage of all data within the school will conform to the EU and UK data protection requirements; Storage of data online, will conform to the EU data protection directive where storage is hosted within the EU.

To ensure the network is used safely, this school:

- Ensures staff read and sign that they have understood the school's online safety Policy. Following this, they are set-up with Internet, email access and network access. The same credentials are used to access the school's network;
- All pupils have their own unique username and password which gives them access to the Internet and other services;
- Makes clear that no one should log on as another user and makes clear that pupils should never be allowed to log-on or use teacher and staff logins;
- Has set-up the network with a shared work area for pupils and one for staff. Staff and pupils are shown how to save work and access work from these areas;
- Requires all users to log off when they have finished working or are leaving the computer unattended;
- Ensures all equipment owned by the school and/or connected to the network has up to date virus protection;
- Makes clear that staff are responsible for ensuring that any computer or laptop loaned to them by the school, is used primarily to support their professional responsibilities.
- Makes clear that staff accessing LA systems do so in accordance with any Corporate policies;
  e.g. Borough email or Intranet; finance system, Personnel system etc.
- Maintains equipment to ensure Health and Safety is followed;
- Ensures that access to the school's network resources from remote locations by staff is audited and restricted and access is only through school/LA approved systems:

- Does not allow any outside Agencies to access our network remotely except where there is a clear professional need and then access is audited restricted and is only through approved systems;
- Has a clear disaster recovery system in place for Admin Files, SIMS and FMS remote off site back up of data;
- This school uses secure data transfer; this includes DfE secure S2S website for all CTF files sent to other schools;
- Ensures that all pupil level data or personal data sent over the Internet is encrypted or only sent within the approved secure system in our LA ;
- Our wireless network has been secured to industry standard Enterprise security level /appropriate standards suitable for educational use;
- All IT and communications systems installed professionally and regularly reviewed to ensure they meet health and safety standards;

Password policy

- This school makes it clear that staff and pupils must always keep their passwords private, must not share with others; If a password is compromised the school should be notified immediately.
- All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password(s) private.
- We require staff to use STRONG passwords.
- We encourage staff to change their passwords regularly.

E-mail

Moreton Church of England Primary School:

- Provides staff with an email account for their professional use and makes clear personal email should be through a separate account;
- We use anonymous or group e-mail addresses, for example admin@moreton.essex.sch.uk.
- Will contact the Police if one of our staff receives an e-mail that we consider is particularly disturbing or breaks the law.
- Will ensure that email accounts are maintained and up to date
- We use a number of technologies to help protect users and systems in the school, including desktop anti-virus products, plus direct email filtering for viruses.

Pupils:

- We are working towards children being given a school e-mail account. This will be an internal account and they will only be able to e-mail each other through this system. Through this they will be taught how to e-mail safely. Any e-Safety concerns are then monitored through the filtering system by the Online Safety Officer/Network Manager.

- Pupils are taught about the online safety and 'netiquette' of using external systems such as e-mailing using a personal account at home.

Staff:

- Staff will use the school e-mail systems for professional purposes
- Access in school to external personal e mail accounts may be blocked
- Never use email to transfer staff or pupil personal data. 'Protect-level' data should never be transferred by email. If there is no secure file transfer solution available for the situation, then the data / file must be protected with security encryption.

School website

- The Headteacher, supported by the Local Governing body, takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained;
- The school web site complies with statutory DFE requirements;
- Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status;
- Photographs published on the web do not have full names attached. We do not use pupils' names when saving images in the file names or in the tags when publishing to the school website;

Cloud Environments

- Uploading of information on the schools' online learning space is shared between different staff members according to their responsibilities e.g. all class teachers upload information in their class areas;
- Photographs and videos uploaded to the school's online environment will only be accessible by members of the school community;
- In school, pupils are only able to upload and publish within school approved 'Cloud' systems.

Moreton Church of England Primary School

Social networking

Staff, Volunteers and Contractors

- Staff are instructed to always keep professional and private communication separate.
- Teachers are instructed not to run social network spaces for student use on a personal basis or to open up their own spaces to their students, but to use the schools' preferred system for such communications. We teach a unit on blogging and social networking in Upper school all of which is monitored by staff.
- for the use of any school approved social networking staff will adhere to school's user agreement. Updates onto our Twitter/Facebook is only allowed by agreed personnel.

School staff will ensure that in private use:

- No reference should be made in social media to pupils, parents/carers or school staff;
- School staff should not be online friends with any current pupil. Any exceptions must be approved by the Headteacher. Staff are advised to protect themselves by exercising caution and carefully consider whether to have ex pupils/parents/carers as 'friends' on social networking sites;
- They do not engage in online discussion on personal matters relating to members of the school community;
- Personal opinions should not be attributed to the school or local authority and personal opinions must not compromise the professional role of the staff member, nor bring the school into disrepute;
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Pupils:

- Are taught about social networking, acceptable behaviours and how to report misuse, intimidation or abuse through our online safety curriculum work.
- Pupils are required to sign and follow our [age appropriate] pupil Acceptable Use Agreement - to be implemented in September 2020.

Parents:

- Parents are reminded about social networking risks and protocols through our parental communications materials when required.
- Are reminded that they need to ask permission before uploading photographs, videos or any other information about other people.

5. Data security: Management Information System access and Data transfer

Strategic and operational practices

At Moreton Church of England Primary School:

- The Finance officer supported by 1159 Production is the Senior Information Risk Officer (SIRO).
- Staff are clear who are the key contact(s) for key school information are.
- We ensure staff know who to report any incidents where data protection may have been compromised.
- All staff are DBS checked and records are held in a single central record

Technical Solutions

- Staff have secure area(s) on the network to store sensitive files.
- We require staff to log-out of systems when leaving their computer, but also enforce lock-out after 10 minutes idle time.
- Our server, portable laptops and iPads are in lockable locations and managed by DBS-checked staff.
- Details of all school-owned hardware will be recorded in a hardware inventory.
- Details of all school-owned software will be recorded in a software inventory.
- Disposal of any equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2006 and/or The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007. Further information can be found on the Environment Agency website.
- Where any protected or restricted data has been held we get a certificate of secure deletion for any server that once contained personal data.

6. Equipment and Digital Content

Mobile Devices (Mobile phones, tablets and other mobile devices)

- Mobile devices brought in to school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally-owned mobile devices.
- Pupils are encouraged not to bring in their own mobile devices; permission should be sought from the Headteacher before any such item is brought in. The School accepts that there may be particular circumstances in which a parent wishes their child to have a mobile phone for their own safety. If pupils bring in their phone they are kept in a secure place by the class teacher until the end of the school day.
- Personal mobile devices will not be used during lessons or formal school time unless as part of an approved and directed curriculum-based activity with consent from Headteacher / SLT.
- Personal mobile devices, which are brought into school, must be turned off (not placed on silent) and stored out of sight on arrival at school. They must remain turned off and out of sight until the end of the day.
- The Bluetooth or similar function of a mobile device should be switched off at all times and not be used to send images or files to other mobile devices.
- Staff members may use their phones during school break times, in the agreed place e.g.. the staffroom. In emergency situations staff may have their phones switched on if they need to take an urgent call; permission needs to be sought from the Headteacher or Deputy Headteacher prior to this.
- All visitors are requested to keep their phones on silent.
- The recording, taking and sharing of images, video and audio on any personal mobile device is to be avoided where possible. Authorised use of video or interactive meetings via zoom/TEAMs is to be recorded. All mobile device use is to be open to monitoring scrutiny and the Headteacher is able to withdraw or restrict authorisation for use at any time, if it is deemed necessary.
- The School reserves the right to search the content of any mobile devices on the school premises where there is a reasonable suspicion that it may contain illegal or undesirable material, including pornography, violence or bullying.
- If a pupil needs to contact his or her parents or carers, they will be allowed to use a school phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office.

Storage, Synching and Access

The device is accessed with a school owned account

- **Teachers will be issued with a mini iPad and laptop for professional use. Some have access to the school camera/video.**
- **The device has a school created account and all apps and file use is in line with this policy. No personal elements may be added to this device.**
- **PIN access to the device must always be known by the network manager. This is not currently the case but will be actioned over the year.**

The device is accessed with a personal account

- **If personal accounts are used for access to a school owned mobile device, staff must be aware that school use will be synched to their personal cloud, and personal use may become visible in school and in the classroom.**
- **PIN access to the device must always be known by the network manager.**
- **Exit process – when the device is returned the staff member must log in with personal ID so that the device can be Factory Reset and cleared for reuse.**

Staff use of personal devices

- Staff handheld devices, including mobile phones and personal cameras must be noted in school – name, make & model, serial number. Any permitted images or files taken in school must be downloaded from the device and deleted on return to school before the device is taken out of the school building.
- Staff are not encouraged to use their own mobile phones or devices in a professional capacity. However, there may be occasions, such as sporting fixtures or for uploading images on to Seesaw/Google Classroom, where they may do so. In these instances, all files need to be uploaded onto the school server once they return to school and immediately deleted from their personal device.
- Mobile Phones and personally-owned devices will be switched off or switched to 'silent' mode. Bluetooth communication should be 'hidden' or switched off and mobile phones or personally-owned devices will not be used during teaching periods unless permission has been granted by a member of the senior leadership team in emergency circumstances.
- If members of staff have an educational reason to allow children to use mobile phones or a personally-owned device as part of an educational activity, then it will only take place when approved by the senior leadership team.
- In an emergency where a staff member doesn't have access to a school-owned device, they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes. Incidents should be reported to the Headteacher / Designated Officer.
- If a member of staff breaches the school policy then disciplinary action may be taken.

Digital images and video

- We gain parental/carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter/son joins the school;
- We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials/DVDs;
- Staff sign the school's Acceptable Use Policy and this includes a clause on the use of mobile phones/personal equipment for taking pictures of pupils;
- If specific pupil photos (not group photos) are used on the school web site, in the prospectus or in other high profile publications the school will obtain individual parental permission for its long term, high profile use;
- Pupils are taught about how images can be manipulated in their online safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children as part of their computing scheme of work;
- Pupils are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.
- Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

Links to other policies:

Code of Conduct

Safeguarding Policy

Curriculum Policy

THIS POLICY HAS BEEN DEVELOPED FROM THE MODEL POLICY PROVIDED BY LGfL.

Moreton Church of England Primary School

Appendix A1: Staff ICT Acceptable Use Agreement

The agreement below is an overview of the acceptable use, by staff, of ICT at Moreton Church of England Primary School. We have an acceptable use agreement to ensure staff are aware of their responsibilities when using ICT. The e-safety and acceptable use policy explains the provision for e-safety throughout the school.

How staff use school ICT

School ICT equipment, including the internet, should be used for school related purposes. Personal use is accepted on the provision usage is in accordance with this agreement, the e-safety policy and deemed reasonable by the deputy or head teacher.

When ICT equipment is to be used, which is not at a fixed location, it is to be booked out using the equipment booking register found in the Resources Room. It is the responsibility of the person returning this equipment to ensure that it is secured safely in the Computing Room.

If laptops, iPads or other mobile devices are to be taken off site this must be agreed by the deputy, headteacher or ICT technician, this is so we know exactly which piece of equipment is where at any time. The exception is the class laptop which may be taken home for staff to work on. County guidance is that laptops and other mobile devices are not to be left in cars unattended.

Child safety

It is our responsibility to educate and support our pupils to use electronic devices and the internet safely. We also have a responsibility to report to the e-safety officer (Computing subject leader, Dianna Brumby) any e-safety issues which will be followed up and acted upon.

Social Networking

Social networking sites must not be accessed in school hours, by staff using the schools facilities, including Wi-Fi. Social networking can be accessed for educational purposes where permission is granted by the deputy or head teacher. e.g. Twitter account to report school sports or snow days, class blog to share children's work. If social networking is to be used age restrictions are to be upheld.

School related business is not to be discussed using social networking; reasonableness is expected when using 'private' or 'direct messaging' as is stated in the Code of Conduct. As a member of the school community we have a responsibility for upholding the Code of Conduct, which states use of social networking must not adversely affect the reputation of the school or bring the school into disrepute.

Befriending of pupils and ex-pupils from our school who are (with the exception of family members) under the age of 18 is not advisable. Befriending of parents is acceptable but discussions of school related business or posting any comments or actions that could adversely affect the school is not acceptable.

E-mail

All e-mails involving school business are to be sent and received using the allocated school e-mail address, unless exceptional circumstances occur. All e-mails from this account are to include a school disclaimer signature at the bottom of the page which will be attached as a template for all e-mails. We can e-mail children from our school but only from and to a school e-mail account.

Moreton Church of England Primary School

Audio, Video and Photography

Audio, video and photographic files remain the property of the school at all times. These are to be stored on the school server or mobile devices (iPad, cameras). These types of files are to be used for school related business; they can be taken and used off site but you are responsible for safe guarding the files and minimising risks.

Only school equipment is to be used by staff for recording audio, video or photographic files. Personal equipment can be used in certain circumstances eg.. football match, however, these images/videos needs to be uploaded to the school server and then deleted from the personal device as soon as is reasonable – this is to safeguard you. You are able to use personal equipment to edit, manipulate and produce resources for these file types but you are responsible for safe guarding the files and minimising risks.

File sharing

File sharing, including the use of removable devices (memory sticks) and cloud based technologies (DropBox), is the responsibility of the user to safeguard the information being used and minimise risks. Encrypted memory sticks can be supplied upon request.

Remote access

We are working towards being able to remotely access the school network from any location but it will be the responsibility of the user to safeguard the information being used and minimise risks. You must ensure that the device in which you are accessing the school network from is up to date with its latest anti-virus and malware software.

Personal Devices

When at school, whilst children are on site (8:45-3:15), personal devices such as mobile phones, tablet computers and laptops should not be used for personal use during direct contact with pupils (teaching times), other than in staff areas e.g. staffroom, office areas. Exceptional circumstances to this should be discussed with the deputy or Headteacher in advance. Personal tablets and laptops can be used for educational purposes but you must ensure that they are free from virus and malware if they are to be connected to the schools network. Please refer to the above section regarding audio, video and photography.

If you have any queries, are unsure of anything or do not have a definitive answer for, please seek advice from Computing Subject Leader or the Deputy Headteacher before proceeding. Any breaches of this agreement, could lead to action under the Disciplinary procedure, including dismissal in serious cases.

I confirm that I have read and understood the above.

Signed …… Date ……

Name (please print) ……

Moreton Church of England Primary School

Appendix A2: Pupil Acceptable Use Agreement

These are the rules I agree to follow when using any digital technology:

- I will ask permission from a teacher before using ICT equipment and will use only my own login and password.
- I will use programs as directed by a teacher or LSA
- To protect myself and other pupils, if I see anything I am unhappy with or receive messages I do not like, I will immediately close the page and tell a teacher or adult.
- I will only access my own file's and not other people's files
- I will ask permission before I send pictures of anyone else
- I will only bring into school portable devices with permission. These can only be used when they have been checked to ensure that they are virus free.
- I will only e-mail people I know, or that my parent/teacher has approved and the messages I send will be polite and sensible.
- I will not give out any personal details ,or arrange to meet someone I have met online.
- When I am using the internet to find information, I will check that the information is accurate as I understand that the work of others may not be truthful.
- I will include a citation if I copy and paste somebody else's text/pictures
- Where work is protected by copyright, I will not try to download copies (including music and videos).
- I will not use my mobile phone in school for any reason. If I do bring my phone to school with me I will follow the school's Mobile Phone Policy.
- If I wear a SMART watch it cannot be connected to the internet and may only be used to tell the time.
- I understand that the school may check my computer files and may monitor the Internet sites I visit.
- If I am involved in incidents of inappropriate behaviour that involve members of the school community (e.g. cyber-bullying, using images/information without permission), the school will take action according the Behaviour Policy.
- I understand that if I do not follow these rules I may not be allowed to use ICT in school and my parents/carers may be contacted

I have read and understood these rules and agree to follow them:

Name:
Class:
Signed:
Dated:

Parent / Carer Countersignature

As the parent / carer of the pupil:

- I know that my child has signed this Acceptable Use Agreement and has received, or will receive, e-Safety education to help them understand the importance of safe use of digital technology– both in and out of school.
- I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems.
- I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the Internet.
- I understand that my child's activity on the ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.
- I will encourage my child to adopt safe use of the Internet and digital technologies at home and will inform the school if I have concerns over my child's e-Safety.

Name of Parent:
Signed:
Dated: