Cottenham Primary School

ICT Acceptable Use Policy

Dated:	Autumn 1 2022
Reviewed by:	Personnel
Next Review date:	Spring 2 2023
Equality Review Checklist	In reviewing this policy due consideration must be given to the impact that changes may have on issues of equality for the protected groups: Age Disability Religion or belief Race Pregnancy and Maternity Sex Sexual orientation Gender reassignment Marriage/civil partnerships If the equality of a protected group is likely to be compromised by changes to the policy then please complete an equality risk assessment and tick here: ☐

COTTENHAM PRIMARY SCHOOL

ICT ACCEPTABLE USE POLICY

The Governing Body is committed to safeguarding and promoting the welfare of children and young people and expects all staff, volunteers and visitors to share this commitment.
This policy should be read in conjunction with our Use of Mobile Phones Policy

Introduction

The purpose of this document is to ensure that all adult users (employees, contractors, secondments, governors, student teachers, volunteers, visitors, invited and supervised community users etc) of Cottenham Primary School's computing facilities are aware of the policies relating to their use. Effective and appropriate use of Information and Communications Technology (ICT) is fundamental to the success and security of the teaching and learning at CPS. In addition, it plays a significant part in maintaining business integrity as well as contributing to business continuity. Misuse of IT systems exposes Cottenham Primary School to liability and loss of reputation. **This policy should be read in conjunction with the ICT Policy, Internet Safety Policy, Confidentiality Policy, Data Protection Policy, Safeguarding and Child Protection Policy, Staff Disciplinary Policy, Data Breach Policy, Information Sharing Framework, and the school's Freedom of Information Publication Scheme.**

Passwords will be withheld by the School Business Manager / ICT Manager preventing access to the network, email system and management information system until it has been confirmed that this document has been read and understood (see form at the back of this policy).

File Server
Access to the server is restricted by username/password. The server is in the locked Library cupboard

The curriculum files are stored on the file server. The School Office files are stored via Central Hosting through ICT Services. No user should have higher permission than 'change'. The ICT Manager should have full access as System Manager to the server.

Back Up File Server
The ICT Manager or other person nominated by the Headteacher should take daily back-ups using a rotation of hard drives based on the following pattern:

MONDAY
TUESDAY
WEDNESDAY
THURSDAY
FRIDAY 1, FRIDAY 2, FRIDAY 3, FRIDAY 4
These removable hard drives must be stored off site in a location agreed by the Headteacher.

Admin PCs
Documents stored on the hard drive (c) of the School Office desktop computers will NOT be backed up via the network. It is therefore prudent for the data owner to ensure a copy is lodged on 'Officeshare' if the data held is sensitive, important or irreplaceable. It is expected practice for School Office staff to file documents within Central Hosting.

Removable Media
Use of Removable Media

- A log of the use of USB sticks will be maintained by the ICT Manager to ensure movement of data is monitored. Staff should **only use an encrypted USB stick provided by the school** and return the memory stick when they no longer need it, or when they leave the employment of the school

- Removable media (USB sticks, hard drives) must be virus checked each time they are installed in a school computer before any data is accessed.
- Removable media must not be used to install unlicensed software on to school computers**.**
- It is the responsibility of the data handler to ensure such data is wiped from the encrypted device immediately it is no longer required.
- NO personal or sensitive data should be stored on home computers, personal phones or other storage devices, or stored on the Portal (Staff Share).

Disposal of Removable Media

- All removable media devices should be wiped free of data and given to the ICT Manager for its safe disposal. This may mean the physical destruction of the device. If a commercial company is used for safe disposal, a certificate must be provided proving its safe disposal.

Disposal of ICT Equipment

Old IT equipment must be disposed of in an environmentally friendly way in liaison with the ICT Manager. Any commercial company undertaking this on the school's behalf should provide a certificate. All data held on magnetic storage devices must be removed before disposal. All assets disposed of should be noted on the Asset Register and first offered to other schools before disposal (if in working order).

Software Licences Log

Software purchased for school use should only be installed on a school computer, with the authority of the ICT Manager. The ICT Manager will maintain a Software License Log detailing the software installed on curriculum and teachers' computers to ensure licences are not breached. This should be audited regularly.

Hardware Inventory

The School Business Manager, in liaison with the ICT Manager and Site Manager, will maintain an inventory of all equipment together with make, model number, serial number, date of purchase and location**.** This will be included on the school's Asset Register.

Network

Only suitably qualified and authorised personnel (i.e. qualified ICT technicians) should make changes to the school's network including the installation of hardware. Such changes should be overseen by the ICT Manager or School Business Manager. Wireless network devices should not be employed unless secured by IT staff qualified to configure such devices.

All such technicians should hold a current DBS certificate and wear a visitor's badge when visiting the school.

A qualified electrician must be used to install all electronic equipment including IWBs.

Only accredited cabling contractors can undertake actions/modifications to the cabling network.

Bromcom

Detailed guidance of how to access Bromcom will be made available to all users. Access will be restricted by password which will be managed by the School Business Manager. Shared use of a username / password could be considered a matter for disciplinary action.

Children's personal details (other than their names) should not be displayed on Interactive White Boards (IWBs).

Physical Security

All IT equipment is to be kept in a secure location, or locking devices used, to prevent opportunist theft. All equipment should be logged on the Asset Register and securely marked.

Screen Savers

The screen savers will appear on a timely basis (as directed by ICT Services/Audit) to prevent a computer being 'left open' and misused by either a member of staff or a pupil. It also protects sensitive data from unauthorised access. Staff should always lock their computer/laptop when leaving it unattended.

All PCs and Central Hosting should be logged out at the end of the day and switched off at the power source.

Use of Usernames & Passwords
The school's policy is that these need to be kept secure and should not be shared with anyone as sharing access compromises the security of the data held on the network and the audit trail of changes.

Passwords should comprise of numbers and letters, and should not be predictable such as a pet's name, holiday destination, maiden name etc. The passwords should be changed regularly in line with the server protocol.

Integrity of passwords for different systems (incl. Bromcom) should be maintained. All passwords must be unique. There should be no 'universal' passwords. Staff must not allow browsers to store passwords for sites containing sensitive information.

The network will lock out after five failed attempts. In such a circumstance, refer to the ICT Manager or the School Business Manager for your password to be reset.

School Laptops
The ICT Manager should keep the local virus checker up to date, particularly when accessing the internet off-site. Each laptop should have an effective firewall and Spyware. All curriculum software installations should go through the ICT Manager and be recorded on the Software Licence Log. All laptops should be encrypted if used off site and storing personal data.

In addition:

- Staff should never leave laptops, devices, ipads or note/netbooks unattended in public places.
- Laptops left in cars are not insured unless they are out of sight in a concealed boot.
- Sensitive documents should be protected by password or encrypted.
- Back ups of data on laptops can be made into the Central Hosting secure area if needed.
- Sophos Anti-virus software runs on the system throughout the school network.
- The County's email system should be used for all school business. Where problems arise, this can be tracked.
- If the use of a memory stick or other removable media has been authorised by the Headteacher, ICT Manager or School Business Manager, the user should connect to the network, click on 'My Computer', right click on the relevant drive and select 'scan with sophos' before accessing or saving the data.
- Laptops are the property of the school and are primarily for delivering school work.
- Family and friends should not be allowed to use the school equipment.
- The member of staff is responsible for maintaining the secrecy of their own password and this should not be divulged to anyone else (including colleagues, pupils or members of their family).
- The member of staff will be held responsible for any misuse of the laptop issued to them.

Staff iPads

- The iPad has been provided by the school for professional use by staff and should not be used by anyone other than the member of staff, including family members
- All staff must set a passcode on their iPad to prevent others from misusing it.
- ITunes account passwords should not be shared with anyone else.

- Staff should not enter/use their own private ITunes account on school ipads.
- Passwords should not be shared - misuse of passwords, codes or other unauthorised access is not acceptable.
- Individual members of staff are accountable for any activity on their mobile devices
- Downloaded apps must be for educational use only e.g. using in school or testing for school
- Use of websites etc. should echo the school's approach to acceptable use of laptops
- Images of pupils should be transferred off the device to the school server before the iPad is taken off site and filed with the current date - see the school's Image Management Protcocol.
- Personal images should not be stored on staff iPads.
- Confidential information should not be stored on staff iPads.
- Accessing inappropriate material – all material on the iPad must adhere to the school ICT Acceptable Use Policy, ie users are not allowed to send, access, upload, download or distribute offensive, threatening, pornographic, obscene, or sexually explicit materials.
- Illegal activities – use of the school's internet/e-mail accounts for financial or commercial gain or for any illegal activity is not allowed.
- Cameras – users must use good judgment when using the camera. The user agrees that the camera will not be used to take inappropriate, illicit or sexually explicit photographs or videos, nor will it be used to embarrass anyone in any way.
- Posting of images/movie on the Internet into a public forum is strictly forbidden, without the express permission of a member of the Senior Leadership team.
- Individual users are responsible for the setting up and use of any home internet connection and no support will be provided for this by the school.

Acceptable Email Use

Use of email by staff is permitted and encouraged where such use supports the success of the teaching and learning at Cottenham Primary School. However, staff members must ensure that, when using the school email system, they:

- use the county's email system;
- comply with current legislation;
- use email in an acceptable way;
- do not create unnecessary risk to the school by their misuse of the Internet.
- Password protect sensitive or personal data sent to an address outside the County's secure email system.

Unacceptable Behaviour

The following are unacceptable:

- use of school email for personal business or to send chain letters or abusive/offensive emails;
- forwarding of school or County confidential messages to external locations and email addresses e.g. Hotmail, Gmail;
- distributing, disseminating or storing images, text or materials that might be considered indecent, pornographic, obscene or illegal;
- distributing, disseminating or storing images, text or materials that might be considered discriminatory, offensive or abusive, in that the context is a personal attack, sexist or racist, or might be considered as harassment;
- accessing copyrighted information in a way that violates the copyright;

- breaking into the school's or another organisation's system;
- unauthorised use of a password/mailbox;
- broadcasting unsolicited personal views on social, political, religious or other non-school related matters;
- transmitting unsolicited commercial or advertising material;
- undertaking deliberate activities that waste staff effort or networked resources;
- introducing any form of computer virus or malware into the school network.

Monitoring

Cottenham Primary School accepts that the use of email is a valuable teaching and learning resource. However, misuse of this facility can have a negative impact upon employee productivity and the reputation of the business and could contravene the UK GDPR**.**

In addition, all the school's email resources are provided for school purposes. Therefore, the school maintains the right to examine any system and inspect any data recorded in those systems with notice.

Content

- E-mail messages must be treated like any other formal written communication.
- Emails may contain personal data and require password protection.
- E-mail messages cannot be considered to be private, secure or temporary.
- Email can be copied and forwarded to numerous recipients quickly and easily and you should assume that they could be read by anyone.
- Improper statements in e-mail can give rise to personal liability and liability for Cottenham Primary School and can constitute a serious disciplinary matter. E-mails that embarrass, misrepresent or convey an unjust or unfavourable impression of Cottenham Primary School or its business affairs, employees, suppliers, parents or pupils are not permitted. Do not create or send e-mail messages that are defamatory. Defamatory e-mails whether internal or external can constitute a published libel and are actionable. Never send confidential or sensitive information via e-mail to a personal account i.e. an account which is not run by a LA service or agency. E-mail messages, however confidential or damaging, may have to be disclosed in court proceedings.
- Do not create or send e-mail messages that may be intimidating, hostile or offensive based on sex, race, colour, religion, national origin, sexual orientation or disability.
- It is never permissible to subject another employee to public humiliation or ridicule; this is equally true via e-mail.
- Copyright law applies to e-mail. Do not use e-mail to transmit or circulate copyrighted materials.

Privacy

- E-mail messages to or from a member of staff cannot be considered to be private or confidential. Although it is not policy to routinely examine the content of individuals' e-mail, Cottenham Primary School reserves the right to monitor messages, at any time, for specific instances in which there is good cause for such monitoring or some legal obligation to do so. Good cause shall include the need to fulfil legislative obligations, detect employee wrongdoing, protect the rights or property of the school, protect IT system security or to comply with legal procedures.
- Messages sent or received may be copied and disclosed by Cottenham Primary School for lawful purposes without prior notice.
- It is not permissible to access or to send e-mail from another employee's personal account either directly or indirectly, unless you obtain that person's prior written approval. Computer (file) storage areas will be treated as school property. The Headteacher, ICT Manager or other staff members with their delegated authority may look at files and communications to ensure that the system, including emails, is being used responsibly.

- Emails have the same legal status as written documents, so the same level of care must be taken.

Sanctions
Failure to comply with these guidelines will result in sanctions ranging from disciplinary procedures such as verbal and written warnings, through to dismissal.

Agreement
All staff members who have been granted the right to use the school's email services are required to sign this agreement (see Appendix A) and confirm their understanding and acceptance of this policy annually.

Instant Messaging
Instant messaging (i.e. chat rooms and services such as MSN and social networking sites such as 'My Space' and 'Facebook', Instagram) carry inherent risks including lack of encryption, logging of chat conversations without a user's knowledge and virus risks. Due to these risks, Cottenham Primary School does not permit its members of staff to use instant messaging for the communication of sensitive or proprietary school information either in or outside school. In addition, members of staff should not accept requests from children to become 'friends' via these sites as such contact is inappropriate, could be misunderstood and is at odds with their professional role in the school.

The Headteacher is responsible for the school's Twitter and Facebook account, if used.

Blogging
Blogging should be done via the school website. Ensure appropriate permissions are observed and data retention protocols followed.

Internet Use
Use of the Internet by members of staff at Cottenham Primary School is permitted and encouraged where such use supports the success of the teaching and learning in school.

However, staff members must ensure that they:
- comply with current legislation;
- use the Internet in an appropriate way;
- do not create unnecessary risk to the school by their misuse of the Internet.

Unacceptable Behaviour
The following is deemed unacceptable use or behaviour by members of staff:
- visiting Internet sites that contain obscene, hateful, pornographic or other illegal material;
- using the computer to perpetrate any form of fraud, or software, film or music piracy;
- using the Internet to send offensive or harassing material to other users;
- downloading commercial software or any copyrighted materials belonging to third parties, unless this download is covered or permitted under a commercial agreement or other such licence;
- hacking into unauthorised areas;
- creating or transmitting defamatory material;
- undertaking deliberate activities that waste staff effort or networked resources;
- introducing any form of computer virus into the school network;
- use of chat rooms;
- submitting images taken at school without permission to a social networking site;
- making comments about school on a social networking site.

Monitoring

Cottenham Primary School accepts that the use of the Internet is a valuable learning resource. However, misuse of this facility can have a negative impact upon use of time and the reputation of the school.

The school maintains the right to monitor the volume of Internet and network traffic, together with the Internet sites visited. The specific content of any transactions will not be monitored unless there is a suspicion of improper use.

Sanctions
Failure to comply with these guidelines will result in sanctions ranging from disciplinary procedures such as verbal and written warnings, through to dismissal or a ban from use of school resources.

Agreement
All school staff members and other members of the school community who have been granted the right to use the school's Internet access are required to sign this agreement (see Appendix A) confirming their understanding and acceptance of this policy.

Removal of Users
The School Business Manager or ICT Manager are responsible for removing email access and Central Hosting access from the Central Hosting Administration Tool for staff (or other members of the school community) leaving Cottenham Primary School.

Procedure if Unacceptable Use Suspected

- No action should be taken directly until the Headteacher has been informed.
- The Headteacher should make arrangements to secure the evidence and the PC should be removed from use.
- Internal Audit, and in serious cases the Police, should be contacted immediately.
- Staff / Management should never attempt to access a site which they believe to be illegal – to do so would technically break the law and make them liable to prosecution. Staff should trust their judgement and quarantine the PC without undertaking any investigations of their own.
- If there is any doubt about the subject matter, it is enough to ***view*** the internet history. Any attempt to follow the internet hyperlinks to the sites themselves will invalidate evidence by updating the time stamps of images received.

IWB Safety Measures
All staff should be aware that it is dangerous to deliberately look into the projector light. Pupils should not be left unsupervised when using projectors. Guidance for use is displayed in all classrooms with IWB (Interactive White Boards).

A qualified electrician must be used to install all electronic equipment including IWBs.

Only accredited cabling contractors can undertake actions/modifications to the cabling network.

Health and Safety - Duty of Care
Where staff work at a computer for long periods, such as in the School Office, regular rest breaks must be facilitated. The cost of eye tests for staff using computers for a large part of their day will be met by the school. Please liaise with the School Business Manager before arranging a test.

Annual self assessment checks should be made by the ICT Manager, monitored by the School Business Manager, as to the positioning of the computer and the seating arrangement for all School Office staff and other staff where the use of computers is considered a significant element of their school day.

Data Security – please see the school's Data Protection Policy

Personal Data and the General Data Protection Regulations (UK GDPR)

Please see the school's Data Protection Policy.
Staff should note that all data and correspondence, including e-mail messages, held by Cottenham Primary School may be provided to the data subject, internal or external, in the event of a subject access request.

Freedom of Information Act – See the school's FOI Publication Scheme

Virus Protection
All computers on the school network are protected by Sophos virus checker which is updated daily through the server.

Care should be taken to avoid this being compromised by introducing removable media to the school network. Where this is considered essential, a scan must be undertaken to ensure the media is virus free (see Use of Removable Media).

Using the internet from a school laptop **at home** is permitted providing the local virus checker (including firewall and spyware) is up to date. (See Internet Use).

Suspicious email attachments from unknown senders must not be opened as they may contain viruses.

Good Housekeeping
It is essential for users to carry out good housekeeping by keeping their files in good order and deleting files no longer current or relevant to hold under UK GDPR, particularly memory hungry files such as video and pictures.

The school's policy for retaining electronic images is for the duration of the child's attendance at Cottenham Primary School plus one year (unless directed otherwise by the parent or the image is one of many in a group photo involving different year groups). Photos will be deleted after that period and if retained for historical purposes only with the parent's consent.

Purchase of New Software/Hardware
All curriculum software will be purchased by the ICT Manager in line with the school's financial regulations, contract regulations and internal procedures. This equipment will be installed and supported by the ICT Manager. The ICT Manager, in liaison with the School Business Manager and Site Manager, is responsible for updating the asset register for any new ICT purchases.

ICT software and hardware for the school administration will be purchased within the school's financial regulations, contract regulations and internal financial procedures and overseen by the School Business Manager and supported by Education ICT Services. The ICT Manager, in liaison with the School Business Manager, is responsible for updating the asset register with any new ICT purchases.

School Website and App
- The school website will be hosted by a third party (Primary Site) using the County's web address www.*cottenham.cambs.sch.uk*.
- The school website will be managed by the School Business Manager/ ICT Manager and overseen by the Headteacher.
- Only images with appropriate parental permissions will be used on the website and such images may be named (first names only) where permissions allow.
- Only work with appropriate parental permissions will be published on the website and such work may be named where permissions allow.
- Staff names and images may be published on the website unless the staff member specifically withdraws permission to do so.

- Access to updating the school website will be available from the school and from another venue off site to provide instant communication where a critical incident needs to be managed away from the site.
- For other image-holding programmes the school utilises, please see the school's Internet Policy.

Appendix A

ICT Acceptable Use at Cottenham Primary School

Name:_____

I have read and understood the Cottenham Primary School ICT Acceptable Use Policy and whilst I am a member of staff at Cottenham Primary School I agree to conduct myself in line with these policy guidelines.

I understand that if I was to fall short of the requirements and expectations highlighted in this policy, this may be deemed as misconduct or gross misconduct and the school's disciplinary procedures would be followed.

I understand that I am asked to confirm this agreement on an annual basis to ensure I continue to be aware of the computer security issues at Cottenham Primary School

Signed:_____

Dated:_____

Appendix B:

Examples of Behaviours which Require the Use of the Disciplinary Policy

GROSS MISCONDUCT Examples

1. Criminal Acts – for example in relation to child pornography

2. Visiting pornographic sites (adult top shelf materials) except where this forms an authorised part of the employees job (for example 'Testing').

3. Harassment – inappropriate e-mails or printed e-mails sent to a colleague, even if sent as a joke. Harassment can take several forms and is defined as unwanted conduct that affects the dignity of people within the workplace.

4. Obscene or racist jokes or remarks which have been shared internally and externally – reflects on the image of employer and brings the organisation into disrepute.

5. Downloading and installation of unlicensed products.

6. Viewing sexually explicit materials, except where this forms an authorised part of the employees job (for example 'Checking a site reported to be unsuitable for pupil viewing').

7. Chat rooms – sexual discourse, arrangements for sexual activity.

8. Violation of Cottenham Primary School's registration with the Federation Against Software Theft – such as software media counterfeiting or illegitimate distribution of copied software.

MISCONDUCT Examples

1 Frivolous use of school computing facilities that risk bringing Cottenham Primary School into disrepute. The distribution of animated Christmas card programmes or 'chain e-mails' beyond the internal e-mail system would represent examples of such misconduct.

2 Entering into contracts via the Internet that misrepresent Cottenham Primary School. Contracts are legally binding agreements and an employee must not enter into any agreements via the Internet to procure goods or services where Cottenham Primary school is liable for this contract, without first consulting Cottenham Primary School's financial procedures (available within the Finance area of the Intranet).

3 Deliberate introduction of viruses to systems.

4 Inappropriate use of social networking sites.