COUNDON COURT

ICT NETWORK POLICY AND USE ACCEPTANCE AGREEMENT

AY2223

Date agreed by Governors:	**September 2022**
Frequency:	**Annually**
Date of next review:	**September 2023**

1. Rationale

The purpose of this policy is to 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.

This policy applies to all members of the Coundon Court community (including staff, students, volunteers, parents/carers, visitors and community users) who have access to and are users of the network, both in and out of Coundon Court.

2. The Curriculum

The curriculum has a clear, progressive online safety education programme as part of the computing curriculum/PSHE and other subject areas. This covers a range of skills and behaviours appropriate to their age and experience.

Online use is age-appropriate and supports the learning objectives for specific curriculum areas.

Student responsibilities are clearly presented in the Acceptable Use Agreement.

Staff will model safe and responsible behaviour in their own use of technology, e.g. use of passwords, logging-off, use of content, research skills, copyright.

Students can only use school-approved systems and publish within appropriately secure / age-appropriate environments.

3. Training

Staff have access to regular training on online safety issues and the school's online safety education program.

All new staff (including those on university/college placement and work experience) are provided with an induction on the Network Policy and the school's Acceptable Use Agreement.

4. Parent awareness

Parents receive information and advice through the website and specific materials as deemed necessary.

5. Expected conduct

All users will use the school IT and communication systems in accordance with the Acceptable Use Agreement. All users will report abuse, misuse or access to inappropriate materials.

Staff, volunteers, and contractors will 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 students have access that is more flexible. They will take professional, reasonable precautions when working with students, i.e. previewing websites before use

and using age-appropriate search engines where more open Internet searching is required.

Parents/Carers will be informed of the User Agreement and policies through the school website.

6. Incident Management

There is strict monitoring and application of the Network Policy and a differentiated and appropriate range of sanctions applied through our behaviour policy.

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.

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 / Social Care will be contacted if one of our staff or students 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.

Our Safeguarding Policy provides clear guidance when managing sensitive incidents. Monthly reports on user activity are received by the Headteacher to monitor for inappropriate use of the network.

7. Network Management

We manage a safe and secure network through the following management strategies.

Internet access, security (virus protection) and filtering

All users are informed that Internet/email use is monitored.

We provide educational filtered secure broadband connectivity.

A filtering system blocks sites that fall into categories (e.g. adult content, race hate, gaming).

Changes to the filtering policy can only be made by the Network Manager.

The Network is protected by anti-virus software.

We use encrypted devices or secure remote access for access to the network on portable devises or from home.

Network management requires, provides or ensures that:

- individual, audited log-ins for all users
- guest accounts occasionally for external or short-term visitors for temporary access to appropriate services
- teacher 'remote' management control tools for controlling workstations/viewing users/setting up applications and Internet web sites, where useful
- a daily back-up of school data (admin and curriculum);
- secure, 'Cloud' storage for data back-up that conforms to DfE guidance;
- and storage of all data within the school will conform to the EU and UK data protection requirements.
- 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. Online access to service is through a unique, audited username and password.
- all students to have their own unique username and password which gives them access to the Internet and other services.
- 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.
- staff are responsible for ensuring that any computer or laptop loaned to them by the school, is used primarily to support their professional responsibilities.
- equipment is maintained to Health and Safety standards.
- access to the school's network resources from remote locations by staff is audited and restricted and access is only through approved systems.
- outside agencies do not access our network remotely except where there is a clear professional need and then access is audited restricted and is only through approved systems.
- there is a disaster recovery system in place that includes a secure, remote off site back up of data.
- there is secure data transfer; this includes DfE secure S2S website for all CTF files sent to other schools.

- all pupil level data or personal data sent over the Internet is encrypted or only sent within the approved secure system.

- The wireless network is secured to industry standard levels appropriate for educational use.

- all IT and communications systems are installed professionally and regularly reviewed to ensure they meet health and safety standards.

8. Password policy

Coundon Court makes it clear that staff and students 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.

We require staff using critical systems to use two factor authentication.

9. E-mail

Coundon Court 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 info@schoolname.la.sch.uk or class e-mail addresses.

Will ensure that email accounts are maintained and up to date.

Email must not 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.

10. School website

The Principal, supported by the 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 students' names when saving images in the file names or in the tags when publishing to the school website.

11. 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, students are only able to upload and publish within school approved 'Cloud' systems.

12. Social networking

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.

School staff will ensure that in private use No reference should be made in social media to students/students, parents/carers or school staff.

School staff should not be online friends with any pupil/student. Any exceptions must be approved by the Principal.

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 /academy 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.

Students:

Are taught about social networking, acceptable behaviours and how to report misuse, intimidation or abuse through our online safety curriculum work.

Students are required to sign and follow our acceptable use agreement.

Parents:

Parents are reminded about social networking risks and protocols through our acceptable use agreement and additional communications materials when required.

13. CCTV

We have CCTV in the school as part of our site surveillance for staff and student safety. The use of CCTV is clearly signposted in the school. We will not reveal any recordings without appropriate permission.

We use specialist lesson recording equipment on occasions as a tool to share best teaching practice. We do not reveal any such recordings outside of the staff and will not use for any other purposes.

14. Data Security

The Principal is the Senior Information Risk Officer. Data Protection breaches / concerns must be reported directly to the Principal.

15. 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.

All servers are in lockable locations and managed by DBS-checked staff.

Details of all school-owned hardware will be recorded in the asset register.

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.

We are using secure file deletion software.

16. Equipment and Digital content

Mobile Devices

Mobile devices brought into school are entirely at the staff member, students & parents or visitor's own risk. The school accepts no responsibility for the loss, theft or damage of any phone or handheld device brought into school.

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 the Principal / SLT.

Student 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.

No images or videos should be taken on mobile devices without the prior consent of the person or people concerned.

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 and non-contact times in private locations.

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, except where it has been explicitly agreed by the Headteacher. Such authorised use is to be recorded. All mobile device use is to be open to monitoring scrutiny and the Principal 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. Staff mobiles devices may be searched at any time as part of routine monitoring.

If a student 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.

Staff use of personal devices

Staff are not permitted to use their own mobile phones or devices in a professional capacity, such as for contacting children, young people, or their families within or outside of the setting.

Staff will be issued with a school phone where contact with students, parents or carers is required, for instance for off-site activities.

Staff should not use personally owned devices, such as mobile phones or cameras, to take photos or videos of students and will only use work-provided equipment for this purpose.

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 and then report the incident with the Principal / 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 and annually.

We do not identify students in online photographic materials or include the full names of students in the credits of any published school produced video materials/DVDs.

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 or pupil permission for its long term, high profile use.

The school blocks/filter access to social networking sites unless there is a specific approved educational purpose.

Students 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.

Coundon Court – Acceptable Use Agreement

This agreement covers use of all digital technologies in school: i.e. **email, Internet, intranet, network resources,** learning platform, software, communication tools, social networking tools, school website, **equipment and systems.**

These rules will help to keep everyone safe and to be fair to others. School systems and users are protected and monitored by security and filtering services to provide safe access to digital technologies.

I will follow 'good practice' advice in the creation and use of my password and change my passwords regularly. If my password is compromised, I will ensure I change it.

I will not allow unauthorised individuals to access my network access, email or hardware.

I will ensure documents, data, etc. are printed, saved, accessed and deleted / shredded in accordance with the school's network and data security protocols.

I will only use the approved email system for school business.

I will not browse, download or send material that is considered offensive or of an extremist nature by the school. I will report any accidental access to, or receipt of inappropriate materials, or filtering breach or equipment failure to the Network Manager.

I will not download any software or resources from the Internet that can compromise the network or might allow me to bypass the filtering and security system or are not adequately licensed.

I will check copyright and not publish or distribute any work including images, music and videos, that is protected by copyright without seeking the author's permission.

I will not connect any device (including USB flash drive), to the network that does not have up to-date anti-virus software.

I will only use school approved equipment for any storage, editing or transfer of digital images / videos and ensure I only save photographs and videos of children and staff on the *appropriate system or staff-only drive within school*.

I will only I take or publish images of staff and students with their permission and in accordance with the school's policy on the use of digital / video images.

I agree and accept that any computer or laptop loaned to me by the school, is provided solely to support my professional responsibilities. It is acceptable to use the equipment for limited personal use, but I will notify the school of any "significant personal use" as defined by HM Revenue & Customs.

I will only access school resources remotely using the school approved system and follow esecurity protocols to interact with them.

I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow school data security protocols when using any such data at any location.

I understand that data protection policy requires that any information seen by me with regard to staff or pupil information, held within the school's information management

system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.