Tupton Hall School

REDHILL ACADEMY TRUST

INFORMATION COMMUNICATION TECHNOLOGY And ONLINE SAFETY POLICY

Approving Body	Governors
Date Approved	TBC……………………………………..
Version	V.6.2
Supersedes Version	V.6.1
Review Date	December 2024

Tupton Hall School
Information Communication Technology and Online Safety Policy

Tupton Hall School is committed to developing the use of ICT throughout the school and to developing the skills and knowledge of parents, staff, students, governors and the wider community.

ICT is used by students to assist their work and learning, by staff as a support to their teaching and administrative work, by support staff to provide effective and efficient support for school systems and procedures and by parents for monitoring students' progress and communicating with school.

Online safety
From this point forward e-safety will be known as online safety.

'For young people ICT is not a novelty but the way they engage with their world - 21st century culture'
(Online Safety Guide)

Online safety encompasses Internet technologies and electronic communications such as mobile phones and wireless technology. It highlights the need to educate children and young people about the benefits and risks of using new technology and provides safeguards and awareness for users to enable them to control their online experiences. The use of new technologies can introduce a number of risks which can be categorised as:

- **Content** - sexual, racist, violent unreliable/bigoted i.e. safety of the mind of the child.
- **Commerce** - scams, phishing and pharming, bluejacking, downloads which steal information.
- **Contact** - via interactive technologies – Instant Messaging, chat and multiplayer games.
- **Culture** - bullying, trolling, camera phones, blogging, moblogging, social networking.

Tupton Hall School has a duty of care, both inside and outside of school, to protect students from these risks. This policy aims to raise awareness of the risks involved when embracing new technologies for Internet safety, Internet security, media literacy and communications.

The ICT and Online Safety Policy will operate in conjunction with a range of other school policies including those for Behaviour for Learning, Bullying, Child Protection and Safeguarding, Curriculum and Teaching & Learning.

The policy as a whole reflects the government guidance in respect of staying safe, being healthy, positive contributions, and achieving economic well-being and enjoyment.

Online safety depends on effective practice at a number of levels:

Responsible ICT use by all staff and students; encouraged by the clarity of the policies and a rigorous approach to training and education to ensure consistency in its application across the school and through school/home links.

Sound implementation of the ICT and Online Safety Policy.

Safe and secure broadband from the East Midlands Broadband Consortium (EMBC/EMPSN) including the effective management of web filtering (Smoothwall, Impero and Senso).

Sexting
The school definition of sexting is 'sending or posting sexually suggestive images, including nude or semi-nude photographs, via social media or over the Internet'. The specific criteria covered by this term are:

- A person under the age of 18 creates and shares sexual imagery of themselves with a peer under the age of 18.
- A person under the age of 18 shares sexual imagery created by another person under the age of 18 with a peer under the age of 18 or an adult.

- A person under the age of 18 is in possession of sexual imagery created by another person under the age of 18.

The law states that it is an offence to possess, distribute, show and make indecent images of children.

All incidents involving youth produced sexual imagery (sexting) will be treated in line with this policy and the school's safeguarding and child protection policies:

- The incident will be referred to the Designated Safeguarding Lead (DSL) (AWE/SBU) as soon as possible.
- The DSL will hold an initial review meeting with appropriate school staff.
- There will be subsequent interviews with the young people involved (if appropriate).
- Parents will be informed at an early stage and involved in the process unless there is good reason to believe that involving parents would put the young person at risk of harm.
- At any point in the process if there is a concern a young person has been harmed or is at risk of harm, further actions in line with the safeguarding policy will take place.
- Any necessary sanctions will be applied in line with the appropriate school policies.

An **initial review** meeting will consider the initial evidence and aim to establish:

- Whether there is an immediate risk to a young person or young people.
- If a referral should be made to the police and/or children's social care.
- If it is necessary to view the imagery in order to safeguard the young person – in many cases, imagery will not be viewed but this may be necessary, and is allowed by the DSL, if it is to establish that the image is inappropriate.
- What further information is required to decide on the best response?
- Whether the imagery has been shared widely and via what services and/or platforms. This may be unknown.
- Whether immediate action should be taken to delete or remove images from devices or online services.
- Any relevant facts about the young people involved which would influence risk assessment.
- If there is a need to contact another school, college, setting or individual.
- Whether to contact parents or carers of the pupils involved - in most cases parents will be involved.

An immediate **referral** to police and/or children's social care may be made if at this initial stage:

- The incident involves an adult.
- There is reason to believe that a young person has been coerced, blackmailed or groomed, or if there are concerns about their capacity to consent (for example owing to special educational needs).
- What the school knows about the imagery suggests the content depicts sexual acts which are unusual for the young person's developmental stage, or are violent.
- The imagery involves under age sexual acts.
- The school has reason to believe a pupil or pupil is at immediate risk of harm owing to the sharing of the imagery, for example, the young person is presenting as suicidal or self-harming.

When the school has decided that other agencies do not need to be involved, then consideration will be given to deleting imagery from devices and online services to limit any further sharing of the imagery.
Students and parents may need reminding that schools have the power to search pupils for devices, search data on devices and delete youth produced sexual imagery.

ALL incidents will be recorded in school and all students involved will be given further guidance on online safety. Appropriate sanctions will be applied in line with the behaviour policy.

Protecting students from online dangers.

There are an increasing number of dangers online. This policy sets out generic advice.

Specific current examples:

Grooming:

The school defines grooming as:

The process by which a person befriends a child to gain his or her trust and to create a situation whereby the child will allow the perpetrator to have sexual contact with him or her and will not tell anyone of it.
Such activity is criminal, and an offence under s.15 of the Sexual Offences Act 2003.

An example of the grooming process:

1. Friendship
Flattering a child into talking in a private chat room where they will be isolated. The child will often be asked for a non-sexual picture of themselves.

2. Forming a relationship
Asking the child what problems they have to create the illusion of being their best friend.

3. Risk assessment
Asking the child about the location of their computer and who else has access to it in order to assess the risk of being detected.

4. Exclusivity
Building up a sense of mutual love and trust with the child, suggesting that they can discuss 'anything'

5. Sex talk
Engaging the child in explicit conversations and requesting sexually explicit pictures from them. At this stage the paedophile will usually try to arrange a meeting with the child.

Grooming is explained to all students through online safety/safeguarding assemblies, is included in the Computing/IT curriculum at all key stages and in the Learning for Life curriculum for some year groups. Educational information is available in school and on the school's website. The school will in all instances work with the appropriate police/social care bodies when instances of grooming are investigated.

Online radicalisation

Terrorist organisations or groups may seek to radicalise and recruit young people through an extensive use of social media and the internet. Tupton Hall has a robust and effective filtering system, which has been reinforced further to detected associated terminology.
We ensure that all staff and students are aware of the risks posed by the online activity of extremist and terrorist groups, through the ICT curriculum and through regular assemblies and other e-safety initiatives.

If staff have a concern for the safety of a specific young person at risk of radicalisation, they should follow the school's safeguarding procedures, including discussing with your school's designated safeguarding lead, and where deemed necessary, with children's social care. The DSL will refer cases to the "Prevent" lead where appropriate or any other appropriate agency.

Writing and reviewing the ICT and Online Safety Policy

The ICT and Online Safety Policy relates to other policies including those for ICT, bullying and for child protection.
The school audits ICT use to establish if the ICT and Online Safety Policy is adequate and its implementation is appropriate.

The Senior Designated Safeguarding Lead (DSL) is the Online Safety Coordinator.
The ICT and Online Safety Policy has been written by the school, agreed by senior leadership and approved by governors.

Roles and responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups at Tupton Hall:
Governors
Governors are responsible for the approval of the ICT and Online Safety Policy and for reviewing the effectiveness of the policy.

Headteacher and Senior Leaders

- The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the Online Safety Co-ordinator.
- The Headteacher and Online Safety Co-ordinator are aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
- The Headteacher/Senior Leadership Team are responsible for ensuring that the Online Safety Coordinator and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Senior Leadership Team will receive regular monitoring reports from the Online Safety Coordinator.

Online Safety Coordinator/Designated Senior Person

- leads on online safety issues
- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies/documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- provides training and advice for staff
- liaises with the local authority/relevant body
- liaises with school technical staff
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments
- meets regularly with Online Safety Governor to discuss current issues, review incident logs and filtering/change control logs
- attends relevant meeting/committee of Governors
- reports regularly to Senior Leadership Team
- works closely with the Senior Assistant Headteacher (Student Experience and Wellbeing).

IT Systems Manager

The IT Systems Manager is responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack.
- that the school meets required online safety technical requirements and any local authority/other relevant body Online Safety Policy/guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed.
- that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant.

- that the use of the network/Internet /remote access/email is regularly monitored in order that any misuse/attempted misuse can be reported to the Headteacher/ Online Safety Coordinator for investigation/action/sanction.
- that monitoring software/systems are implemented and updated as agreed in school policies.

Teaching and support staff

Teaching and Support Staff are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current school Online Safety Policy and practices.
- they have read, understood and signed the Staff Acceptable Use Agreement.
- they report any suspected misuse or problem to the Headteacher/Online Safety Coordinator for investigation/action/sanction.
- all digital communications with students/parents/carers should be on a professional level and only carried out using official school systems.
- online safety issues are embedded in all aspects of the curriculum and other activities.
- students understand and follow the online safety and acceptable use agreements.
- students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices.
- in lessons where Internet/Wi-Fi/phone/tablet use is pre-planned students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in Internet searches

Child protection / Designated Safeguarding Lead (DSL)

The DSL– Senior Assistant Headteacher (Wellbeing) is also trained in online safety issues and is aware of the potential for serious child protection/safeguarding issues to arise from:

- sharing of personal data
- access to illegal/inappropriate materials
- inappropriate online contact with adults/strangers
- potential or actual incidents of grooming
- cyber-bullying

Students:

- are responsible for using the school's digital technology systems and other devices (including their own) in accordance with the Student Acceptable Use Agreement.
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking/use of images and on cyber-bullying.
- should understand the importance of adopting 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, if related to their membership of the school.

Parents/Carers

Parents/carers play a crucial role in ensuring that their children understand the need to use the Internet/mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website, specific training events and information about national/local online safety campaigns/literature. Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events.
- access to parents' sections of the website and online student records.
- their children's personal devices in the school.

Community users

Community users who access school systems/website as part of the wider school provision will be expected to sign a Community User Acceptable Use Agreement before being provided with access to school systems, including the Wi-Fi.

ICT – Administration

ICT will be used wherever possible to assist staff in their roles and responsibilities, to provide data as appropriate and to assist in the management of school systems, e.g. finance, attendance, performance monitoring.

The IT Systems Manager in conjunction with the Senior Leadership Team, will be responsible for all aspects of ICT administration and cross-school procurement.

ICT – Curriculum

ICT will be used wherever possible to assist staff and students in their teaching and learning. The Head of Computing in conjunction with other key staff will be responsible for co-ordinating all aspects of ICT in the curriculum.

There are a number of ICT facilities located around the school. There are two specialist ICT rooms, two Sixth Form ICT suites, and six of the faculties each take part-responsibility for one ICT suite each. The library also has a suite of PCs with faculty and year areas also have clusters of PCs in work rooms. There are an increasing number of wireless laptop trolleys (14 at present) in school and as the network further develops, access to ICT resources will continue to increase.

The school operates an open door policy in the two specialist ICT rooms. Other ICT rooms are available for similar use with permission from the IT Systems Manager or the relevant Faculty Manager.

All staff should be aware that these resources are also available at all times for their own use, timetable allowing.

PC rooms that are not timetabled may be booked centrally or in specific faculties.

Technician support is available for the majority of the working week. This can be utilised (with appropriate prior notice to the IT Systems Manager) to assist with the preparation of materials to assist the teaching of subjects using Information Technology.

Problems with machines do occur and can be minimised if staff and students take care of the resource, use careful time management and planning. Problems in rooms should be reported to the ICT Help Desk using either e-mail, electronic reporting system, by phone or in person.

Those problems requiring more immediate intervention should initially be reported immediately to a technician via the ICT Help Desk in order that help can be given and the operation of the resource can be managed effectively.

A number of INSET and specific training opportunities will continue to be offered. Bespoke training is available for teaching and support staff, once arranged with the IT Systems Manager. The Senior Assistant Headteacher responsible for Continuing Professional Development (CPD) is responsible for ICT INSET.

Software and licensing

Software used on school ICT resources must be purchased with an accompanying individual or site licence. This means that the software is licensed for use (either unlimited or limited to a number of machines at any one time) on the school site only, unless exceptions are specified within the licence.

The exception to the above rule is where a member of staff is allowed one copy of a current Microsoft desktop operating system and one copy of the current Microsoft Office software for use at home on their personal computer for the duration of their contract, or the duration of the licence.

Software is available from the IT Systems Manager or the IT Help Desk and must be signed for.

Additional licences may be purchased by the school where colleagues are required to undertake work at home on specific software. The IT Systems Manager will monitor and authorise all requests for such software.

Any software purchases should firstly be discussed with the IT Systems Manager and when the software arrives in school it should be registered centrally with the IT Systems Manager for secure storage/installation.

Software audits will be carried out on a regular basis to ensure no unlicensed software is being used in school. Software is installed on the server which will:

- Prevent programs from being downloaded from the Internet.
- Audit all software on network connected machines via the server.

A rolling programme of audits will continue on stand-alone machines and all other equipment.

Faculty Leaders who are concerned that unlicensed software might be being used in their area should discuss the matter with the IT Systems Manager.

Under no circumstances must copies of any software be transferred to or from any off site system.

Software is continually being updated and a catalogue of available software is being developed and is available upon request from the IT Systems Manager.

CDs etc. of purchased software must be given to the IT Systems Manager on receipt and original copies of licences etc. will also be kept by the IT Systems Manager.

The IT Systems Manager will maintain an inventory of software installed and will monitor the licencing requirements, purchasing additional when required in discussion with the SLT.

Internet

Internet access will be available to staff and students via all workstations connected to the school network where considered appropriate, after an agreement has been signed.

All members of the school community and visitors to the school are expected to use the Internet in an appropriate manner at all times and ‘Internet Use Guidelines’ will be displayed in all areas. Staff are expected to sensibly use the Internet and should broadly comply with the student 'Rules for the use of the Internet'.

Students will be educated in the effective use of the Internet for research including the skills of knowledge location and retrieval. Evaluation of online materials is a part of teaching and learning across the curriculum, students will be expected to acknowledge the sources of information and to respect copyright.

All use of the Internet by students, staff and other users will be monitored and users will be made aware of the monitoring procedure.

If students or staff discover unsuitable material, the URL and the nature of the content should be reported immediately to the IT Systems Manager or ICT Help Desk.

Any unsuitable URL or site deemed inappropriate by our Internet Service Provider or Internet filter provider, will be automatically banned. The ICT Help Desk is happy to ban or monitor sites at the request of teaching staff.

Where staff feel inappropriate sites or material have been accessed, they should report it to the IT Systems Manager.

Where staff feel sites that have valid appropriate learning material have been blocked, they can request the site to be unblocked by the IT Systems Manager. Site access will only be granted once it has been fully explored and its content checked.

Students are not allowed to access chat rooms although access is permitted to monitored user groups where students and staff are involved in specific projects (e.g. forums and wikis), or via user groups within Tupton Hall micro sites. Staff will discuss the issues relating to the use of chat rooms to highlight potential dangers as part of the core ICT programme of study.

Any member of the school community or other school user who, in the opinion of the Senior Leadership Team or the IT Systems Manager, uses the Internet inappropriately will have their Internet access rights removed. The Headteacher may, in such cases, carry out disciplinary procedures.

The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer.

Rules for the use of the Internet.

- The student must access the Internet only for study purposes or for school-authorised/supervised activities.
- Students must not use the Internet to obtain, download, send, print, display or otherwise transmit or gain access to materials that are unlawful, obscene or abusive.
- Students are expected to respect the work and ownership rights of people outside the school as well as students and staff. This includes abiding by copyright laws.
- Students must not engage in chat activities over the Internet. This takes up valuable resources that could be used by other people for to benefit their studies.
- Students will not give personal information such as their addresses or telephone number to those who they contact through electronic mail.

Classroom Internet control

The school will ensure that staff are trained to use Impero and Senso Consoles to monitor student activity in the classroom, block Internet access for the whole class or individuals or limit activities to set URLs (website addresses).

Impero and Senso Consoles sre available in all ICT classrooms and can be used across the whole network.

Community use of the Internet

The school will provide a username and password for when guests arrive wishing to use ICT facilities. Access to shared drives will only be granted with specific permission of the IT Systems Manager.

The school will provide community Internet access for students and guests to access the Internet within the school environment using their own devices – laptop PC, tablet PC or mobile phone using the school's full wireless network.

This access is monitored by the schools internet filter Smoothwall.

Email

Email is an essential means of communication for both students and staff. Students and staff are encouraged to use approved email accounts on the school system. A school based **@tuptonhall.org.uk** address is provided to all users, personal email addresses should not be used for school communication.

Emails containing confidential data should be sent using encryption protocols provided by the Service Host (Microsoft) to ensure that the potential for any data breach is minimised.

The school operates a single sign on (SSON) facility for access to the school email facility. All users must log off of the computers they are using in school when finished to preserve the security of their email accounts.

Access to the school email system at home is granted through the THS-Portal, school website and via Office.com.

Staff using mobile devices to access their school e-mail must ensure that these devices are kept secure and automatically lock. Devices should ideally have a complex pin number (6 or more digits) and/or use biometric security built into the device.

Students must immediately tell a teacher if they receive offensive email.

Students must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission.

Students who infringe their Internet access privileges will be dealt with in line with the school's Behaviour for Learning policy.

Emails will be scanned, content which is unsuitable will not be sent and a copy of the offending email forwarded to the IT Systems Manager for follow up with the Headteacher.

The contact details on the website should be the school address, email and telephone number. Staff or students' personal information must not be published.

Internet and email personal use and monitoring definitions

Personal use

- Limited personal use of email and the Internet is allowed. But be reasonable. Limited use means no more than a few minutes a day to respond to urgent incoming personal mail.
- Where possible, personal use of the email system should be in your own time.
- All personal access to the Internet must be in your own time. You can use the Internet before you start work, during your lunchtime, or after work.
- If you buy something on the Internet be careful. The school/county council will not accept any liability.
- Use your common sense. Excessive personal use will stop you doing your job. It may also result in disciplinary action and the loss of your email and Internet access.

Monitoring

- All staff and students will be made aware of how THS monitors Internet and email use by staff training, ICT lessons, assemblies and this policy booklet.

- We will carry out random checks to rule out excessive personal, illegal or inappropriate use of our email and Internet systems.
- Mistakes do happen. If you have visited a 'banned' website or received an inappropriate email – please report the incident to the IT Systems Manager
- The 'Smoothwall' web filter monitors Internet use, requests to sites are scanned, and inappropriate sites blocked. This is an active filter that continuously scans, monitors and learns from sites to update the block list effectively.
- 'Smoothwall' is supported in school by 'Senso', this is used to actively monitor Internet usage in school. The software will alert class teachers to inappropriate student use of the Internet. System administrators are also alerted to any inappropriate use by any user.
- Logs generated by 'Senso' will be interrogated to track past usage for all users and will be used as evidence in cases of misuse.
- email is filtered by our online email host (Microsoft) using the 'Forefront' software. All incoming and outgoing traffic is scanned for viruses and the following is logged. email logs will only be interrogated by the IT Systems Manager when potential breaches of school policy or safeguarding need investigating:

    - The email address of the person sending the email.
    - Your email address and those of any other recipients.
    - The size and name of any attachments.
    - Date and time sent.
    - The text of the email.

THS-Portal/ Home Access+

Access to staff and students' work and email is provided via the THS-Portal and Home Access+. These portals allow access to users’ documents and resources using a secure websites utilising users’ school log-on credentials.

Use of this facility is provided subject to the terms set out in this policy for use of the network.

In Touch/ClassCharts

A texting service that allows Tupton Hall School staff to send secure text and e-mail messages.

ClassCharts has become the schools preferred method of communication to parents, students and staff. It allows push notices as well as messages in from parents.

Both of these allow the school message about a whole range of school matters, ranging from times for trips, clubs and activities, attendance issues, bullying and event reminders.

Managing emerging technologies

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed. This includes devices used to access our wireless network.

Mobile phones/MP3 players and other devices

Mobile phones and other 4G/wireless devices cannot be used in school as explained in school mobile phone policy.

Reviews of the mobile phone policy will be undertaken in response to changes in technology and emergent technologies.

Publishing students’ images and work

Photography and video (images) are used at school for a number of reasons, including:

- Sharing students’ achievements
- Recording of school events
- Providing display materials
- Publicity purposes (brochures, leaflets, media articles, website and social media*)

Due to the way we share information across multiple platforms, consent applies to all of the above. E.g. a printed prospectus may also be published on the school website, school news article may also be shared on Facebook and Twitter.

*Our school currently uses Facebook, Twitter and Instagram

Parents/carers can object to students' images being used by completing the parental agreement attached to the Student Computer and Internet Policy or at any time by contacting the school directly. Objections will be indicated on SIMS.Net. Staff have access to an up-to-date list of objections on the staff drive.

We **do not** require consent to use images of students for the following reasons:

- To support staff CPD and training
- Evidencing students’ learning and progress for internal or external assessment
- Safeguarding reasons

In order to avoid them being identified by anyone who does not already know them, a child’s full name will not be used alongside their image in any promotional material published outside of school, unless parental permission has been granted.

Where an image featuring a group of children is published, their full names may appear in the accompanying text but not in a way that would lead to them being identified by anyone who does not already know them.

Staff or students wishing to use personal photographic equipment when recording school events will be required to use memory card devices supplied by the school.

Images taken on personal mobile devices will be transferred to the school’s secure network and removed from the device as soon as possible after use.

MS Teams and Video Confessing

The emergence of the Covid pandemic has brought the use of teams to the forefront in how lessons can taught remotely. Teams allow staff to setup groups of students allowing teaching and learning conversations and video conferenced lessons.

Video conferencing enables users to see and hear each other between different locations. This ‘real time’ interactive technology has many uses in education. Video conferencing may be used in school in accordance with the guidelines below.

- External IP addresses will not be made available to other sites.
- Video conferencing contact information will not be put on the school website.
- Students will ask permission from a teacher before making or answering a video conference call.
- Video conferencing will be supervised appropriately for the students’ age and ability.
- If third party materials are to be included, check that recording is acceptable to avoid infringing the third party intellectual property rights.
- Establish dialogue with other conference participants before taking part in a video conference. If it is a non-school site it is important to check that they are delivering material that is appropriate for your class.

Protecting personal data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 and General Data Protection Regulations (GDPR).

School data will not be taken off site using memory sticks, flash drives or any other portable media unless the device is encrypted by the ICT Help Desk.

Staff laptops will be encrypted using BitLocker to secure any data in the event of loss, theft or damage.

Hard drives will be disposed of securely with certificates of data destruction obtained.

Where possible access to data using services provided by the THS-Portal should be from Staff Laptops which comply with encryption requirements to minimise data breaches.

Where this is not possible, any data or documents downloaded to a private device are the responsibility of that member of staff.

- It must be kept in in a secure folder on the device or an encrypted Zip file.
- Once used it must be uploaded back to the schools servers and all copies deleted with recycle bins emptied.

Storage and use of biometric data.

Staff and parents/carers of students will initially be given the opportunity to opt into the submission of their staff/students' biometric identity for storage by the school. This data will be used for the sole purpose of authenticating or registering access to school systems.

The biometric system used will generate a template of biometric Identities in such a form that it can not be reverse-engineered to recreate the original information.

By signing either the school's Employee Internet and Email Policy or the Tupton Hall School Computer and Internet Policy staff or parents of students agree to the storage of a biometric template and the use thereof.

Alternate arrangements will be provided to any individual that does not consent to the processing of their biometric information that allow the individual to access relevant services.

Online safety complaints and ICT abuse / online safety infringement consequences

Online safety complaints will be processed as set out in the guidelines below.

- Complaints about Internet misuse will be dealt with under the school’s complaints procedure.
- All online safety complaints and incidents will be recorded by the school, including any actions taken.
- All members of the school community will need to be aware of the importance of confidentiality and the need to follow the official school procedures for reporting concerns.
- Any issues (including sanctions) will be dealt with according to the school’s disciplinary, Behaviour for Learning and child protection procedures.
- All members of the school community will be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the school community.

Depending upon the severity of the first offence the Senior Leadership Team will discuss the offence and issue a warning to the student. The offence will be logged in the behaviour management system.

For serious offences the evidence will be collated and a letter sent home describing the offence committed with associated evidence. This will be accompanied by a telephone call home. Students will have their Internet access terminated for a period of time. This may also prevent the student from accessing files held on the system including examination coursework. All information will be logged into the behaviour management system.

The Designated Safeguarding Lead (DSL) will be informed of any online safety incidents involving Child Protection concerns, which will then be dealt with appropriately.

Where online safety has been breached more than once, further sanctions in conjunction with the school Behaviour for Learning Policy will apply.

Wireless network

The school has a full site-wide wireless network. This policy applies to all aspects of the wireless network.

Staff and students will have full access to the wireless network. It will operate as if part of the main network.

Visitors may use the 'Guest' wireless to access the Internet.

The 'Guest' wireless may also be used by students and staff using their own laptops and mobile devices. Students and staff using this facility will have normal monitored access to the Internet and may access their normal resources through the THS-Portal.

ALL devices used to connect to the 'Guest' wireless may be accessed by the ICT Help Desk to note Media Access Control (MAC) addresses to ensure security.

Introducing the ICT and Online Safety Policy to students

- Online safety rules/advice will be posted in all networked rooms and other classrooms where mobile laptop computers are used.
- Students will be informed that network and Internet use will be monitored.
- The ICT and Online Safety Policy will be available for all to access.

Staff and the Online Safety Policy

All staff will be given the school Online Safety Policy and its importance explained.

Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

Staff should read and understand this policy and the ICT and Online Safety booklet.

Staff and students will be reminded not to leave work stations logged on. The school is considering introducing automatic log-off to stop this problem.

Enlisting parents' support

Parents' attention will be drawn to the school ICT and Online Safety Policy in newsletters, the school prospectus and on the school website.

Internet issues will be handled sensitively to inform parents without undue alarm.

Parents interested in child online safety matters will be referred to organisations such as CEOP (Child Exploitation and Online Protection). The link to this is on the school website.

Advice will be given to parents about filtering systems and responsible Internet use upon request and online safety workshops will be advertised to parents.

ICT security and inventories

The ICT Systems Manager is responsible for the security of both the Local Area Network (LAN) and Wide Area Network (WAN).

The use of user logins and complex passwords to access the school network will be enforced. Complex passwords will be required to consist of 8 or more characters, with one upper case, one lower case and a digit.

Personal data sent over the Internet is encrypted using Secure Socket Layer (SSL) certificates from **GlobalSign**.

All computers and associated items will be security marked by the ICT Help Desk team wherever possible. An additional identification mark will also be added to the computers to facilitate the monitoring of individual machines.

Items should be entered on curriculum area inventories as appropriate as well as the whole school ICT inventory maintained by the IT Systems Manager. Where possible serial numbers should be recorded for all items.

The whole school ICT inventory will provide an overview of all resources within the school and provide a profile of each machine.

Insurance

The school has insurance to cover the theft of hardware and software from the premises only.

All staff and students are encouraged to adopt practices which will encourage good security of rooms and equipment.

Staff wishing to continue curriculum development or professional development by making use of school owned systems outside school hours and off the premises should first discuss the matter with the IT Systems Manager or the Business Manager.

Colleagues are advised to check car and home insurance policies to ensure they are adequately covered for any loss or damage prior to using personal items at home.

Laptops are covered by the same rules as above. Staff with a school laptop must sign an agreement form. Staff laptops when covered by an agreement form are covered by the county council insurance policy. Also staff should ensure they do not leave laptops in vehicles.

Damage and protection

Any staff member detecting any damage or malfunction should report it directly to the IT Systems Manager or ICT Help Desk as soon as it has been detected.

Effective virus protection software is installed on the school network. If, however, staff find anything strange about the PCs after memory sticks, CDs, DVDs brought into school have been used, they should report it to the IT Systems Manager or ICT Help Desk.

Every ICT user, member of staff and student has a responsibility to the whole ICT user community.

Authorisation and access

Levels of access will be established for different users on the various networks and systems operating in school.

Responsibility for maintaining and monitoring access and authorisation will be as follows:

School Network	IT Systems Manager in consultation with the Senior Leadership Team.
Broadband connections	IT Systems Manager in consultation with the Senior Leadership Team.
Sims.Net and Sims Learning Gateway management system	IT Systems Manager and Data Manager in consultation with the Senior Leadership Team and Business Manager

All access and authorisations will be limited to nominated personnel and details of passwords and other secure information will be kept by the IT Systems Manager, under guidance from the Senior Leadership Team.

All staff will follow established ICT guidelines on using passwords effectively and where LEA guidelines exist, users will follow those guidelines, e.g. SAP finance system.

Access to the servers is limited to nominated personnel: IT Systems Manager and ICT Help Desk team under guidance of the IT Systems Manager.

Cybersecurity and Cyber Attacks

The school will endeavour to safeguard all users and devices against cyberattacks by.

- keeping its virus and malware protection updated to the latest definition versions
- Regularly scanning of all its devices and the monitoring of the results in SCCM console.
- Updating the school firewalls to the latest versions in order to prevent against Denial of Service and emerging Malware issues.
- Keeping devices up to date with security patches.
- Advising all users on potential emerging threats.
- Reviewing the run only GPO policy assigned to students as new software is required.

However it is everyone's responsibility to guard against potential Cyber incidents by staying vigilant and not opening suspect emails or files.

However as threats are continually changing, should there be cybersecurity issue, the School will follow the plan set out in the ICT Disaster Recovery plan for returning to normal service levels.

Backing up

The IT Systems Manager will ensure that regular and systematic back-up of data is completed on a regular basis so that recovery of essential data can be managed in the event of loss of data files or system failure.

Back-up copies will be securely stored against theft, corruption or physical damage so that in the event of a major incident a back-up copy is available.

A 30 day back-up process is in place to guard against data loss, this process is mirrored in Azure cloud backup where a 7 day, 3 week backup is kept off site.

Disaster recovery procedures

The school will ensure procedures are in place to recover all data and return ICT systems to full use in the event of a critical incident or local problem. RAID mirroring and RAID striping ensures data is not lost in the event of main server failure and software is available to recover data from individual machines.

The IT Systems Manager will maintain:

1. An up to date list of contacts who will be available to assist in the recovery process, e.g. network management consultants, key staff, suppliers.
2. A list of procedures and action required by key individuals in the event of a critical incident.

A copy of these lists is kept by the IT Systems Manager and the Business Manager.

CCTV System Policy

Updated November 2021

Introduction

The purpose of this policy is to regulate the management, operation and use of the closed circuit television (CCTV) system at Tupton Hall School. This policy follows the Data Protection Act 2018 and General Data Protection Regulations (GDPR) guidelines.

The system comprises of a number of fixed and remote direction controlled cameras located around the site along with a recording and management suite, which is password protected.

The CCTV system is owned and maintained by Interserve Support Services and will only be available to authorised staff as listed.

- Headteacher.
- Senior Leadership Team Members.
- Business Manager.
- Premises Manager (Interserve Support Services).
- Network Manager.

CCTV Objectives

- To protect the school buildings and their assets.
- To increase personal safety and reduce the potential from crime.
- To support the Police in deterring and detecting crime.
- To assist in identifying, apprehending and prosecuting offenders.
- To protect members of the public and private property.
- To assist the management of the school.

Intent

- The CCTV Scheme is registered with the Information Commissioner under the terms of the Data Protection Act 2018 and GDPR and will comply with the requirements of the Data Protection Act, GDPR and the Commissioner's Code of Practice.
- The school will treat the system and all information, documents and recordings obtained and used as data which are protected by the Act and GDPR.
- Cameras will be used to monitor activities within the school and its car parks and other public areas to identify criminal activity actually occurring, anticipated, or perceived, and for securing the safety and wellbeing of the school, together with its visitors.
- Staff have been instructed that static cameras are not to focus on neighbouring properties.
- Materials or knowledge secured as a result of CCTV will not be used for any commercial purpose. Recordings will only be released to the media for use in the investigation of a specific crime and with the written authority of the police. Recordings will never be released to the media for purposes of entertainment.

- The planning and design has endeavoured to ensure that the system will give maximum effectiveness and efficiency, however it is not possible to guarantee that the system will cover or detect every single incident taking place in the areas of coverage.
- Warning signs, as required by the Code of Practice of the Information Commissioner have been placed at all access routes to areas covered by the school CCTV.
- A log will be kept of Authorised Staff access to Recorded Images.

Operation and Access

- The Scheme will be administered and managed by the Headteacher, in accordance with the principles and objectives expressed in the code.
- The day-to-day management will be the responsibility of the Business Manager with the assistance of the ICT Technical Team when required.
- Images can be accessed only on the PC which is authorised for such use. Currently, this is limited to the PC in the Comms Room, which is password protected. Other staff maybe invited to view the images to aid identification.
- Live feeds and recording play back from each camera are also available in main reception from the CCTV recorder control console. Live feeds are available to authorised school staff for the management of the school, security of the site and safety of staff and pupils.
- The CCTV system will be operated 24 hours each day, every day of the year.
- CCTV recordings will be available for 30 days unless copied to removable media (CD's, DVD's or Tapes etc). After this period any recordings will be automatically erased.

Printed and Recording Media Procedures

In the event of an incident requiring footage from the system to be retrieved and stored the following procedure should be followed:-

- The details of the incident should be passed to the Business Manager, who will authorise the use of the system by an authorised user.
- The relevant footage will be identified.
- An entry shall be made on the Recorded Image Viewing Log.
- If the footage is required for investigation then the User will produce a copy. The Date and Time of the recorded extract will be registered and stored in a secure place and retained in line with school policy.
- The footage may only be viewed by Authorised Staff.
- Subsequent requests to view the footage will be approved to interested parties only (senior School staff, police and parents)
- A record of all viewings shall be made, which if required as evidence, may be released to the Police.
- Applications received from outside bodies (e.g solicitors) to view or release records will be notified to the Headteacher who will document his decision.

Assessment of the System

- The Business Manager will check and confirm the efficiency of the system daily and in particular that the equipment is recording to a high quality and that cameras are fully functional.
- Regular reviews of the system's operation will take place and any necessary changes in procedure and camera sighting/position will be implemented
- If out of hours emergency maintenance arises, the Business Manager must be satisfied of the identity and purpose of contractors before allowing entry.

Breaches of the code (including breaches of security)

- Any breach of the Code of Practice by school staff will be initially investigated by the Headteacher, in order for him/her to take the appropriate action.

- Any serious breach of the Code of Practice will be immediately investigated and an independent investigation carried out to make recommendations on how to remedy the breach.
- Breaches will be reported to the Information Commissioners Office in line with the schools data protection policy.

Complaints

- Any complaints about the school's CCTV system should be addressed to the Headteacher or Business Manager.
- Complaints will be investigated in accordance with the schools complaints procedures. 10.

Access by the Data Subject

- The Data Protection Act provides Data Subjects (individuals to whom "personal data" relate) with a right to data held about themselves, including those obtained by CCTV.
- Requests for Data Subject Access should be made on application via the school reception using the appropriate Subject Access Request form.

Summary of Key Points

- This Policy will be reviewed every two years.
- The CCTV system is owned and operated by Interserve Support Services.
- The CCTV system will not be permanently manned.
- The CCTV system is not open to visitors except by prior arrangement and good reason.
- Recording media will be used properly indexed, stored and destroyed after appropriate use.
- Media may only be viewed by Authorised School Staff and third parties authorised by the head teacher.
- Media required as evidence will be properly recorded witnessed and packaged before copies are released to the police.
- Media will not be made available to the media for commercial or entertainment.
- Media will be disposed of securely.
- Any Covert Surveillance or use of a Covert Human Intelligence Source being considered or planned as part of an operation must be authorised in writing by the Headteacher.
- Any breaches of this code will be investigated by the Headteacher.
- Breaches will be reported to the Information Commissioners Office in line with the schools data protection policy.
- Breaches of the code and remedies will be reported to the Headteacher.

EMPLOYEE IT, INTERNET & EMAIL POLICY

Updated November 2022

All staff have access to the Internet. In school access to the Internet is provided for the purposes of educational research and learning, and for access to email. The purpose of this policy is to provide rules for appropriate use of the Internet. All employees who wish to use the Internet in school should carefully read, sign and return the following agreement to the IT Systems Manager so that can then be stored in your records.

EMPLOYEE AGREEMENT

I understand that access to the Internet from Tupton Hall School must be in support of educational research or learning, and I agree to the following:

- I will use the Internet and email for school use only. I understand that I may use the facilities for personal use in accordance with personal use definitions.
- I will refrain from accessing any instant messaging, blogs, social media, web pages or other areas of cyberspace that would be considered offensive in the judgement of the school's Headteacher (or delegate) because of pornographic, racist, violent, illegal, illicit or other content.
- Accordingly, I am responsible for monitoring and appropriately rejecting materials, links, dialogues and information accessed/received by me and the students I am supervising.
- I will not use valuable Internet time playing non-educational games, or trading.
- I will be courteous and use appropriate language. I will refrain from using obscene, harassing or abusive language and will report any cases of such usage against me to the Senior Leadership Team.
- I appreciate that other Internet users might have different views from my own and I will therefore conduct myself appropriately and professionally at all times whilst in the cyber community.
- I accept responsibility to keep copyrighted material from entering the school. Therefore I will not download software, games, music, graphics, videos or text materials that are copyrighted. I will not violate any copyright laws by posting or distributing copyrighted materials.
- Plagiarism is unacceptable. Therefore I will use any downloaded material in an appropriate manner in work, listing its source in a bibliography and clearly specifying any directly quoted material.
- I will not reveal personal information, including names, addresses, credit card details and telephone numbers of staff or students at Tupton Hall School.
- I am aware that the use of **social networking** and **instant messaging sites** should be carefully thought through. I am aware that I should NOT use such sites for personal reasons during normal working hours. I understand that I am extremely vulnerable if I allow access to private data and am aware that I am STRONGLY advised to keep private information secure, and NOT to add students as 'friends' on such sites. If students are allowed access to my social networking site and inappropriate information or images are accessible, I understand that I will be asked to remove the material and may be in breach of this policy.
- I will not damage computers, computer systems or networks. Furthermore, if I discover any methods of causing such damage I will report them to the Senior Leadership Team and I will not demonstrate them to others.
- I will abide by the current sign-on procedures for access to the computer network.
- I acknowledge that, while questionable material exists on the Internet, the user must actively seek it and therefore is ultimately responsible for bringing such material into the school. I therefore do not hold the staff or Headteacher of Tupton Hall School responsible for any such materials acquired from the Internet.
- I understand that the failure to abide by this Employee Internet Policy may result in professional disciplinary action being taken against me by the Headteacher and Governors, and/or prosecution.

- I understand that the school may keep my **biometric details** and agree to the use of this data for the sole purpose of verifying access to school systems.
- I understand that it is my responsibility to protect against Cyber Attacks and will not knowingly open any potentially dangerous emails and/or files on school devices.
- I will seek help immediately from the ITC Helpdesk if I think I have opened a potentially dangerous email and/or file on school devices.

STAFF AGREEMENT

I hereby acknowledge that I have read the agreement on staff use of computers and the Internet at Tupton Hall School. I have read the ICT and Online Safety Policy and Social Media policies.

I understand that access is designed for educational purposes. I recognise that, while efforts will be made to monitor use of computers and Internet, it is impossible for Tupton Hall School to continually monitor and restrict access to all controversial materials. I further acknowledge that, while questionable material exists on the Internet, the user must actively seek it and therefore is ultimately responsible for bringing such material into the school. I therefore do not hold Tupton Hall School responsible for any such materials acquired from the Internet.

I am happy for the school to collect, store and share data about me and my contacts in accordance with the Staff Privacy Notice. □

Name (please print name) ……………………………………

Signed …………………………………………………………

Date ………………………….

STUDENT IT, INTERNET & EMAIL POLICY

Updated November 2022

The School's computer network is well established and plays a big part in the education of students and others at Tupton Hall. In school access to the Internet is provided for the purposes of educational research and learning.

STUDENT AGREEMENT

I understand that access to the Internet from Tupton Hall School must be in support of educational research or learning, and I agree to the following:

- I will refrain from accessing instant messaging, blogs, social media, web pages or other areas of cyberspace that would be considered offensive in the judgement of the school's Headteacher (or delegate) because of pornographic, racist, violent, illegal, illicit or other content.
- I will not use chat rooms unless as part of a teacher-led educational project.
- I will not knowingly allow links, websites or messages of an offensive or dangerous nature into school.
- I will not use valuable Internet time playing non-educational games.
- The school has effective web content filtering, but not all offensive material will automatically detected. I will not try to cheat the filtering system, and search for information of an offensive nature.
- I will be courteous and use appropriate language. I will refrain from using obscene, harassing or abusive language and will report any cases of such usage against me to my teacher or the Senior Leadership Team.
- I accept responsibility to keep copyrighted material from entering the school. Therefore, I will not download software, games, music, graphics, videos or text materials that are copyrighted. I will not violate any copyright laws by posting or distributing copyrighted materials.
- Plagiarism is unacceptable. Therefore, I will use any downloaded material in an appropriate manner in assignments, listing its source in a bibliography and clearly specifying any directly quoted material.
- I will not reveal personal information, including names, addresses, credit card details and telephone numbers of others or myself.
- I will not damage computers, computer systems or networks. Furthermore, if I discover any methods of causing such damage I will report them to the Senior Leadership Team and I will not demonstrate them to others.
- I will not attempt to change any computer, monitor or software settings on any school computers.
- I will abide by the current sign-on procedures for access to the computer network, respect other students' work and not attempt to access other people's work on the network by using either aliases or passwords that are not mine.
- The entire network is protected by anti-virus software. Students and staff are advised to use anti-virus software on home computers and laptops. If a virus is reported on screen, a member of ICT staff should be informed immediately.
- The IT Systems Manager carries out daily network backups. I will, however, attempt to save my own work correctly, and use sensible file management techniques at all times.
- I will refrain from cyber-bullying of any form.
- I will use the school email and other email sensibly and not breach any of the points in this agreement.
- I will only use my mobile phone, laptop and/or other device in accordance with the school rules and with permission of the specific teacher in lessons.
- I will not use my mobile phone or any other device to record video, take digital photographs, or edit digital images of staff, students or any other person without their prior consent.
- I understand that images of students and staff will be taken in accordance to the reasons set out in the ICT and Online Safety Policy.
- I understand that the school may keep my **biometric details** and agree to the use of this data for the sole purpose of verifying access to school systems.

- If I violate any of the terms of this agreement, I will be denied access to the Internet and/or computers for a time to be determined by the Headteacher and may face further disciplinary action as determined by the Headteacher. I am aware that each case will be considered on its merits.
- I understand that it is my responsibility to protect against Cyber Attacks and will not knowingly open any potentially dangerous emails and/or files on school devices.
- I will seek help immediately from the ITC Helpdesk if I think I have opened a potentially dangerous email and/or file on school devices.

TUPTON HALL SCHOOL COMPUTER AND INTERNET POLICY

PARENTAL AGREEMENT

I hereby acknowledge that I have read the agreement on student use of computers and the Internet at Tupton Hall School. I have read the ICT and Online Safety Policy and have discussed both with my child.

I understand that access is designed for educational purposes. I recognise that, while efforts will be made to monitor student use of computers and Internet, it is impossible for Tupton Hall School to continually monitor and restrict access to all controversial materials. I further acknowledge that, while questionable material exists on the Internet, the user must actively seek it and therefore is ultimately responsible for bringing such material into the school. I therefore do not hold the staff or Headteacher of Tupton Hall School responsible for any such materials acquired from the Internet.

I am happy for the school to retain any biometric information regarding my son/daughter. □

Parent/carer name (please print) ………………………………………………………………………….

Child name ………………………………………………………………………… Form ……………………….

Signed ………………………………………………………………………… Date ………………………………

PLEASE RETURN THIS FORM TO SCHOOL

Tupton Hall School Cookies Policy

Updated November 2021

Our website www.tuptonhall.org.uk uses cookies. By using our website you consent to our use of cookies in accordance with the terms of this policy.

About cookies

A cookie is a file containing an identifier (a string of letters and numbers) that is sent by a web server to a web browser and is stored by the browser. The identifier is then sent back to the server each time the browser requests a page from the server.

Cookies can be used by web servers to identity and track users as they navigate different pages on a website and identify users returning to a website.

Cookies may be either 'persistent' cookies or 'session' cookies.

A persistent cookie consists of a text file sent by a web server to a web browser, which will be stored by the browser and will remain valid until its set expiry date (unless deleted by the user before the expiry date).

A session cookie, on the other hand, will expire at the end of the user session, when the web browser is closed.

Our cookies

We only use session cookies on this website.

We will send you the following cookies:

popup	Sets internet popups top false.	false	24 Hours
MUID		348399498212652C317289A5835F64D3	24 Hours

Third party and analytics cookies

When you use our website, you may also be sent third party cookies.

We may use Google Analytics to analyse the use of this website. Google Analytics generates statistical and other information about website use by means of cookies, which are stored on users' computers. The information generated relating to our website is used to create reports about the use of the website. Google will store this information. Google's privacy policy is available at: http://www.google.com/privacypolicy.html.

Cookies and personal information

Cookies do not contain any information that personally identifies you, but personal information that we store about you may be linked, by us, to the information stored in and obtained from cookies.

Blocking cookies

Most browsers allow you to refuse to accept cookies. For example:

1) in Internet Explorer (version 11) you can block cookies using the cookie handling override settings available by clicking 'Tools', 'Internet Options', 'Privacy' and then 'Advanced';
2) in Firefox (version 51) you can block all cookies by clicking 'Menu', 'Preferences', 'Privacy', selecting 'Use custom settings for history' from the drop-down menu, and un-ticking 'Accept cookies from sites';
3) in Chrome (version 56), you can block all cookies by accessing the 'Customise and control' menu, and clicking 'Settings', 'Show advanced settings' and 'Content settings', and then selecting 'Block sites from setting any data' under the 'Cookies' heading.

Blocking all cookies will, however, have a negative impact upon the usability of many websites.

If you block cookies, you may not be able to use all the features on this website.

Deleting cookies

You can also delete cookies already stored on your computer. For example:

1) in Internet Explorer (version 11), you must manually delete cookie files by clicking on the settings cog, selecting 'Safety' then clicking 'Delete Browsing History'.
2) in Firefox (version 51), you can delete cookies by clicking 'Firefox Button', 'History', 'Clear Recent History'.
3) in Chrome (version 56), you can delete all cookies by accessing the 'Customise and control' menu, and clicking 'Settings', 'Show advanced settings' and 'Clear browsing data', and then selecting 'Delete cookies and other site and plug-in data' before clicking 'Clear browsing data'.

Again, doing this may have a negative impact on the usability of many websites.

Contact us

This website is owned and operated by Tupton Hall School.

If you have any questions about our cookies or this cookies policy, please contact us:

By Email - enquiries@tuptonhall.derbyshire.sch.uk
By telephone - 01246 863127

Tupton Hall School Laptop Policy

Updated February 2021

This Laptop Ref: **THSXXXX** has been configured with access to the whole school network, and to the laptop itself.

You are responsible for this laptop until you have had **TWO COPIES** of this form **signed as returned by a member of the ICT Team.**

Instructions on how to save between the laptop and the network are included with the case.

Keeping virus software up to date should be an automated process once online, however if you have problems with this process, please inform a member of the ICT team. At various intervals, maintenance will be undertaken; when software not licensed to the school may be removed if necessary.

A member of the ICT team will authorise any software or Internet connections required by a user once license authenticity has been established. Under no circumstances should you install unlicensed software on this computer, by doing so you may be breaking the law. If any unlicensed software is found, it will be deleted and may be reported to the Headteacher.

The licensing agreement for school-owned laptops insists that all staff are aware that laptops must ONLY be used for school based work. Any work carried out on school-owned software must only be used for school purposes.

The laptop is a curriculum resource and should be used, in accordance with the school Internet Policy, and ICT Policy.

If a third party Internet connection has been installed then during the laptop's regular inspection Internet usage will be examined. If any inappropriate Internet content is found then it will be fully documented and may be reported to the Headteacher. This is in accordance with the school's Internet usage policy.

When the laptop is returned; either permanently of for maintenance, it should be done so with the AC adapter, the power cable, and the case.

The laptop remains school property and as such is covered by school insurance, as long as it has not been left in a vehicle.

Name: ……………………………………………………………………………………

Signed: ……………………………………………………………………………………

Date: ……………………………………………………………………………………

RETURNED	
CHECKED	
DATE	

For assistance with any laptop issues, please talk to a member of the ICT Help Desk team.

Staff Agreement for use of Software at Home

Updated February 2017

Microsoft Open Value Subscription for Education Solutions.

As part of our school's agreement, any member of staff who works more than 200 hours per year is entitled to install (for their own use) one copy of both MS Windows 8 Professional and MS Office 13 Professional. This is on the understanding that upon termination of your contract with the school or on termination of the licence contract, the software will be completely uninstalled from any PC/laptop that you own.

Office for Mac is also available.

We also have a licence which covers the following software for home use. Any members of staff wishing to install these products are subject to the same conditions of use as above.

Adobe CC (50 copies only)
Macromedia Fireworks.
Macromedia Flash.
Macromedia Dreamweaver.

By signing this agreement you are agreeing to comply with the terms of use set out above.

Microsoft Open Value Subscriptions for Education Agreement

I agree to the terms and conditions set out above for installation of any one or more of the products listed above on one home computer or laptop that I own.

Name ______________________________

Date ______________________________

Signature ______________________________