	Name of School	**Coteford Infant School**
	Policy review Date	**04.10.2019**
	Date of next Review	**04.10.2020**
	Who reviewed this policy?	**Mary Myzer: Computing Co-ordinator.**

This policy is part of the School's Statutory Safeguarding Policy. Any issues and concerns with online safety must follow the school's safeguarding and child protection processes.

Contents

Appendices (separate documents):

A1: Acceptable Use Policy (Staff, Volunteers and Governors)

A2: Acceptable Use Policy (Pupils)

A3: Acceptable Use Policy including photo/video permission (Parents/carers)

A4: Protocol for responding to online safety incidents
http://www.ticbradford.com/downloads/esafeguarding/teachers/216-first-line-information-support-for-esafety-incidents/file - handling infringements
http://www.ticbradford.com/downloads/esafeguarding/teachers/216-first-line-information-support-for-esafety-incidents/file - page 23 onwards

A5: Prevent: Radicalisation and Extremism

A6: Data security: Use of IT systems and Data transfer

Search and Confiscation guidance from DfE
https://www.gov.uk/government/publications/searching-screening-and-confiscation

A7: Policy Infringements

IT equipment Receipt Form

A8: VPN Setup form

1. Introduction and Overview

Rationale

The purpose of this policy is to:

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

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

Content

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

Contact

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

Conduct

- Aggressive behaviours (bullying)
- Privacy issues, including disclosure of personal information
- Digital footprint and online reputation
- Health and well-being (amount of time spent online, gambling, body image)
- Copyright (little care or consideration for intellectual property and ownership)

Scope

This policy applies to all members of **Coteford Infant School** community (including staff, pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of **Coteford Infant School** IT systems, both in and out of **Coteford Infant school.**

Roles and responsibilities

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

Role	Key Responsibilities
	• Take day to day responsibility for online safety issues and a leading role in establishing and reviewing the school's online safety policy/documents • Promote an awareness and commitment to online safety throughout the school community • Ensure that online safety education is embedded within the curriculum • Liaise with school technical staff where appropriate • To communicate regularly with SMT and the designated online safety Governor/committee to discuss current issues, review incident logs and filtering/change control logs • To ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident • To ensure that online safety incidents are logged as a safeguarding incident • Facilitate training and advice for all staff • Oversee any pupil surveys / pupil feedback on online safety issues • Liaise with the Local Authority and relevant agencies • Is regularly updated in online safety issues and legislation, and be aware of the potential for serious child protection concerns.
Governors/Safeguarding governor (including online safety)	• To ensure that the school has in place policies and practices to keep the children and staff safe online • To approve the Online Safety Policy and review the effectiveness of the policy • To support the school in encouraging parents/carers and the wider community to become engaged in online safety activities
Computing Curriculum Leader	• To oversee the delivery of the online safety element of the Computing curriculum
Network Manager/technician	• To report online safety related issues that come to their attention, to the Online Safety Coordinator • To manage the school's computer systems, ensuring - school password policy is strictly adhered to. - systems are in place for misuse detection and malicious

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

Role	Key Responsibilities
	• To model safe, responsible and professional behaviours in their own use of technology
Pupils	• Read, understand, sign and adhere to the **Pupil Acceptable Use Policy** prior to commencing the school. • To understand the importance of reporting abuse, misuse or access to inappropriate materials • To know what action to take if they or someone they know feels worried or vulnerable when using online technology • To understand the importance of adopting safe behaviours and good online safety practice when using digital technologies out of school and realise that the school's online safety policy covers their actions out of school • To contribute to any 'pupil voice' / surveys that gathers information of their online experiences
Parents/carers	• To read, understand and promote the school's **Pupil Acceptable Use Policy** with their child/ren • to consult with the school if they have any concerns about their children's use of technology • to support the school in promoting online safety and endorse the **Parent/Carer Acceptable Use Policy** which includes the pupils' use of the Internet and the school's use of photographic and video images
External groups including Parent/Carer groups	• Any external individual/organisation will sign an **Acceptable Use Policy** prior to using technology or the Internet within school • to support the school in promoting online safety • To model safe, responsible and positive behaviours in their own use of technology.

Communication:

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

- Policy to be posted on the school DB Primary pages in the **Staffroom Community** and **Parent/Carer community** and to be distributed by email to all Staff and Governors and kept in the Policy folder. Policy to be part of school induction pack for new staff with a copy of the Staff Handbook.
- Regular updates and training on online safety for all staff.
- Acceptable Use Policies discussed with staff and pupils at the start of each year.
- Acceptable Use Policies to be issued to whole school community, on entry to the school.

Handling Incidents:

- The school will take all reasonable precautions to ensure online safety.
- Staff and pupils are given information about infringements in use and possible sanctions.
- ***Head Teacher*/*Designated Safeguarding Lead*** acts as first point of contact for any incident.
- Any suspected online risk or infringement is reported to ***Headteacher*/*Designated Safeguarding Lead*** that day
- Any concern about staff misuse is always referred directly to the ***Headteacher***, unless the concern is about the ***Headteacher,*** in which case the compliant is referred to the ***Chair of Governors*** and the LADO (Local Authority's Designated Officer).
- The LADO could also be involved when dealing with incidents involving staff.

Review and Monitoring:

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

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

2. Education and Curriculum

Pupil online safety curriculum

This school:

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

Staff and governor training

This school:

- makes regular training available to staff on online safety issues and the school's online safety education program;
- provides, as part of the induction process, all new staff with information and guidance on the **Online Safety Policy** and the school's **Acceptable Use Policies**.

Parent/Carer awareness and training

This school:

- provides induction for parents/carers which includes online safety;
- runs a rolling programme of online safety advice, guidance and training for parents/carers.

3. Expected Conduct and Incident management

Expected conduct

In this school, all users:

- are responsible for using the school IT and communication systems in accordance with the relevant **Acceptable Use Policies**;
- understand the significance of misuse or access to inappropriate materials and are aware of the consequences;

- understand it is essential to reporting abuse, misuse or access to inappropriate materials and know how to do so;
- understand the importance of adopting good online safety practice when using digital technologies in and out of school;
- know and understand school policies on the use of mobile and hand-held devices including cameras;

Staff, volunteers and contractors

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

Parents/Carers

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

Incident Management

In this school:

- there is strict monitoring and application of the online safety policy and a differentiated and appropriate range of sanctions, see appendix 7, Policy infringements;
- all members of the school are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the school's escalation processes;
- support is actively sought from other agencies as needed (i.e. the local authority, LGfL, UK Safer Internet Centre helpline, CEOP, Prevent Officer, Police, IWF) in dealing with online safety issues;
- monitoring and reporting of online safety incidents takes place and contribute to developments in policy and practice in online safety within the school;
- parents/carers are specifically informed of online safety incidents involving young people for whom they are responsible;
- the Police will be contacted if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law;
- we will immediately refer any suspected illegal material to the appropriate authorities – Police, Internet Watch Foundation and inform the LA.

4. Managing IT and Communication System

Internet access, security (virus protection) and filtering

This school:

- informs all users that Internet/email use is monitored;
- has the educational filtered secure broadband connectivity through the LGfL;
- uses the LGfL filtering system which blocks sites that fall into categories (e.g. adult content, race hate, gaming). All changes to the filtering policy are logged and only available to staff with the approved 'web filtering management' status;
- ensures network health through use of Sophos anti-virus software (from LGfL);
- Uses DfE, LA or LGfL approved systems including DfE S2S, LGfL USO FX2, Egress secure file/email to send 'protect-level' (sensitive personal) data over the Internet
- Uses encrypted devices or secure remote access where staff need to access 'protect-level' (sensitive personal) data off-site;

Network management (user access, backup)

This school

- Uses individual, audited log-ins for all users - the LGfL USO system;
- Uses guest accounts occasionally for external or short-term visitors for temporary access to appropriate services;
- Ensures the Systems Administrator/network manager is up-to-date with LGfL services and policies/requires the Technical Support Provider to be up-to-date with LGfL services and policies;
- Has daily back-up of school data (admin and curriculum);
- Uses secure, 'Cloud' storage for data back-up that conforms to DfE guidance;
- Storage of all data within the school will conform to the EU and UK data protection requirements; Storage of data online, will conform to the EU data protection directive where storage is hosted within the EU.

To ensure the network is used safely, this school:

- Ensures staff read and sign that they have understood the school's online safety Policy. Following this, they are set-up with Internet, email access and network access. Online access to service is through a unique, audited username and password. We also provide a different username and password for access to our school's network.
- All classes have their own unique username and password which gives them access to the Internet and other services; Pupils are allocated with their own unique username and password to DB Primary, Mathletics and Doodle Maths (KS1 only).

- Makes clear that no one should log on as another user and makes clear that pupils should never be allowed to log-on or use teacher and staff logins;
- Has set-up the network with a shared work area for pupils and one for staff. Staff and pupils are shown how to save work and access work from these areas;
- Requires all users to log off when they have finished working or are leaving the computer unattended;
- Ensures all equipment owned by the school and/or connected to the network has up to date virus protection;
- Makes clear that staff are responsible for ensuring that any computer, tablet or laptop loaned to them by the school, is used primarily to support their professional responsibilities.
- Maintains equipment to ensure Health and Safety is followed;
- Ensures that access to the school's network resources from remote locations by staff is audited and restricted and access is only through school/LA approved systems:
- Does not allow any outside Agencies to access our network remotely except where there is a clear professional need and then access is audited restricted and is only through approved systems;
- Has a clear disaster recovery system in place that includes a secure, remote off site back up of data;
- This school uses secure data transfer; this includes DfE secure S2S website for all CTF files sent to other schools;
- Ensures that all pupil level data or personal data sent over the Internet is encrypted or only sent within the approved secure system in our LA or through USO secure file exchange (USO FX);
- Our wireless network has been secured to industry standard Enterprise security level /appropriate standards suitable for educational use;
- All IT and communications systems installed professionally and regularly reviewed to ensure they meet health and safety standards;

Password policy

- This school makes it clear that staff and pupils must always keep their passwords private, must not share with others; If a password is compromised the school should be notified immediately.
- All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password(s) private.
- We require staff to use STRONG passwords contacting a mixture of letters and numbers
- We require staff to change their passwords into the MIS, LGfL USO admin site and to the school's network twice a year.

E-mail

This school

- Provides staff with an email account for their professional use, London Staffmail/LA email and makes clear personal email should be through a separate account;
- Staff also have access to an internal mail system as part of the Online Learning Platform **(DB Primary).** This mail system is used only to develop Curriculum needs and not a method of communication between staff, parents/carers and children to discuss specific educational needs.
- We use a google account to manage the networking of our wireless devices using the domain @cotefordinfantschool.co.uk. These accounts are not used for email.
- We use an anonymous email account for general enquiries, which is directed to the admin team: office@coteford-inf.hillingdon.sch.uk
- Will contact the Police if one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law.
- Will ensure that email accounts are maintained and up to date
- We use a number of LGfL-provided technologies to help protect users and systems in the school, including desktop anti-virus product Sophos, plus direct email filtering for viruses.
- Staff can access their LGfLmail on their personal mobile phones, as long as the device is password protected.

Pupils:

- We use an internal mailing system as part our Online Learning Platform **(DB Primary).**
- Pupils are taught how to use the mail system and communicate with peers as part of the curriculum in Year 2 as well as 'netiquette' of using e-mail both in school and at home.

Staff:

- Staff use the LGfLmail systems at school.
- Staff will use LA or LGfLmail for professional purposes.
- Access in school to external personal email accounts may be blocked
- Never use email to transfer staff or pupil personal data. 'Protect-level' data should never be transferred by email and a secure document transfer system (USO FX) is used if data needs to be transferred.
- Staff must not use children's full names in emails to Third Parties and, in compliance to GDPR 2018, if referring to a child to another professional, staff must only use their initials and date of birth to identify them.

School website:

- The Headteacher, 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 pupils' names when saving images in the file names or in the tags when publishing to the school website. Photographs of children will only be published on the website for up to 3 years and then they will be removed from the website public view and media storage.

Learning Platforms and Cloud Environments

DB Primary

- The school uses DB Primary as our Online Learning Platform, which is accessed by Staff, Pupils, Governors and Parents/Carers.
- All users have a Unique Sign On (USO) and accounts are password protected. Accounts are set up by the Office Manager when the community member joins the school as part of the joining process. Accounts also decommissioned by the Office Manager when the member leaves.
- 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;
- Pupils accounts have an online function that alerts the Admin user and their class teacher if they see any contact that is worrying to them.

Social networking

For the purposes of this policy, Social Media is any type of interactive online media that allows parties to communicate instantly with each other or to share data in a public forum. This includes online social forums such as Twitter, Facebook and LinkedIn, Instagram, YouTube and Flickr amongst others.

Coteford Infant School currently does not have any social media sites it is affiliated with, but does recognise that parents and carers have set up their own unofficial sites on Facebook and WhatsApp as a means of communication, of which the school does not take responsibility for.

The Parent Staff Association (PSA) own a Facebook page which is carefully moderated by the Chair of the PSA in line with this policy.

Staff, Volunteers and Contractors

- Staff are instructed to always keep professional and private communication separate.
- Caution is advised when inviting work colleagues to be 'friends' in personal social networking sites; Social networking sites blur the line between work and personal lives and it may be difficult to maintain professional relationships or it might be embarrassing if too much personal information is known in the work place.
- Teachers are instructed not to run social network spaces for pupil use on a personal basis or to open up their own spaces to their pupil, but to use the schools' preferred system for such communications such as *DB Primary*.

Private use of Social Media for School staff and volunteers

The aim of this policy is to advise staff and others of the expectation of working in a school environment when using social media, and highlighting:

1. The importance of ensuring that relevant privacy settings are activated and regularly reviewed.
2. The restrictions of maintaining a professional relationship and professional conduct are adhered to.
3. Guidance on what is acceptable and what is unacceptable when using social media.

Therefore, school staff and volunteers will ensure that in private use:

- They are not be online friends with any pupil. Any exceptions must be approved by the Head Teacher.
- The school will encourage them to check their privacy settings for their personal social media account accounts regularly to ensure they are aware of who can see their data.
- Staff are not allowed to access their personal social media websites from the School's computers or devices at any time unless written consent has been obtained from the Headteacher. As such, steps have been taken to restrict access to sites such as Twitter, Facebook and other social media websites on its computers.
- staff may wish to use their own computers or devices, such as laptops and smartphones, to access social media websites whilst they are at work but must limit use to their official rest breaks such as their lunch breaks.
- Staff are permitted to say that they work for the school, which recognises that it is natural for its staff to sometimes to want to discuss their work on social media. However, the staff member's online profile (for example, the name of a blog or a Twitter name) must not contain the School's name (for example e.g. @Mrs_Brown_Coteford is not allowed). Staff should not accept a "friend" request from a parent or carer connected to the school who is only known to the staff member as the result of a professional relationship.

- Caution is exercised when accepting online "friend" requests or similar with parents of children at the school and that always, personal opinions should not be attributed to the school or local authority and must not compromise the professional role of the staff member. This includes:

1. **Bringing the school into disrepute, for example by:**
    - Having any contact with pupils' family members through social media if that contact is likely to constitute a conflict of interest or call into question their objectivity;
    - Criticising or arguing with parents, colleagues etc;
    - Making defamatory comments about individuals or other organisations or groups;
    - Posting images that are inappropriate or links to inappropriate content;
    - Giving personal contact details to children or young people, including their mobile telephone number or personal email address;
    - Using personal equipment (e.g. mobile phone device) to communicate with children or young people;
    - Not having the relevant written permission from parents for communication, using the School's equipment. Permission must detail the specific reasons why this communication is required;
    - Making contact for personal reasons;
    - Using the internet or other communication channels to send personal messages to children/young persons;
    - Responding to/ request personal information from a child or young person, other than that which might be appropriate as part of your professional role;
    - Mentioning in a negative manner, the School its pupils, parents or colleagues;
    - Commenting on any incidents that occur or have occurred within the School;
    - Posting photographs, videos or any other types of image of pupils and their families;

2. **breaching confidentiality, for example by:**

    - Discussing confidential or personal information about an individual (such as a colleague or pupil) or organisation (such as a supplier of services);
    - Discussing the School's internal workings (such as ongoing Personnel issues, or its future business plans that have not been communicated to the wider public);
    - The School does not expect staff members to discontinue contact with their family members via personal social media once the School starts providing services for them. However, any information staff members obtain in the course of their employment must not be used for personal gain nor be passed on to others who may use it in such a way;
    - School or email addresses and other official contact details must not be used for setting up personal social media accounts or to communicate through such media;

3. **Do anything that could be considered discriminatory against, or bullying or harassment of, any individual, for example by:**

    - Making offensive or derogatory comments relating to age, disability, gender reassignment, race (including nationality), religion or belief, sex and sexual orientation;
    - Using social media to bully another individual (such as a staff member of the school); or

- Posting images that are or are likely to be considered discriminatory or offensive;
- Using social media and the internet in any way to attack, insult, abuse or defame pupils, their family members, colleagues, other professionals, other organisations.

4. **Breach copyright, for example by:**

    - Using someone else's images or written content without permission;
    - Failing to give acknowledgement where permission has been given to reproduce something

Pupils:

- Are taught about social networking, acceptable behaviours and how to report misuse, intimidation or abuse through our online safety curriculum work.
- Pupils are required to sign and follow Pupil Acceptable Use Policy.

Parents/Carers:

- Parents/Carers are reminded about social networking risks and protocols through our Parent/Carer Acceptable Use Policy and additional communications materials when required.
- Are not permitted to upload any photographs or videos to any social media sites. Any exceptions must be approved by the Head Teacher.

CCTV

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

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

Strategic and operational practices

At this school:

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

Technical Solutions

- Staff have secure area(s) on the network to store sensitive files.
- We require staff to log-out of systems when leaving their computer, but also enforce lock-out after 20 minutes idle time.

- We use the LGfL USO Auto-update, for creation of online user accounts for access to broadband services and the LGfL content.
- All servers are managed by DBS-checked staff.
- Details of all school-owned hardware will be recorded in a hardware inventory.
- Details of all school-owned software will be recorded in a software inventory.
- Disposal of any equipment will conform to The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007. Further information can be found on the Environment Agency website.
- Where any protected or restricted data has been held we get a certificate of secure deletion for any server that once contained personal data.

6. Equipment and Digital Content

School Equipment

School Laptops and tablets:

Staff may be issued with a laptop or tablets, which they are allowed to use at home. They will be required to sign an agreement (see appendix 8: IT equipment issue agreement) to ensure they take care of the school equipment, server and data that is carried on the laptop. It will be issued by the Technician and the staff member's name added to the global inventory list, kept on the server in the protected Technician's folder. Teachers are responsible for the care and usage of school equipment at home. School equipment must be password protected at all times and if passwords are changed by staff, they must inform the technician immediately.

Personal Laptops:

Staff are permitted, with permission from the Headteacher, to connect to the server from home using their school laptop or a personal laptop, as long as protocols have been agreed and an agreement signed (see appendix 9: VPN setup form) which states:

1. The device has a secure password.
2. The device has appropriate anti-virus software installed (approved by the technician)
3. Permission has been granted by the Headteacher.
4. An agreement has been signed by staff member, headteacher and technician with details of the End User agreement.

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

- Mobile devices brought into school are entirely at the staff member, pupils & parents/carers or visitors own risk. The School accepts no responsibility for the loss, theft or damage of any phone or hand held device brought into school.
- No pupil should bring his or her mobile phone or personally-owned device into school. Any device brought into school will be confiscated.

- Mobile devices are not permitted to be used in pupil changing rooms and toilets.
- Personal mobile devices will not be used during lessons or formal school time unless as part of an approved and directed curriculum-based activity with consent from Headteacher / SMT.
- 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 Head Teacher. Such authorised use is to be recorded. All mobile device use is to be open to monitoring scrutiny and the Headteacher is able to withdraw or restrict authorisation for use at any time, if it is deemed necessary. Exceptions would be for parents/carers during school assemblies or performances, where they will also have to follow the social media policy.

Staff use of personal devices

- Mobile Phones and personally-owned devices will be switched off or switched to 'silent' mode and will not be used during teaching periods unless permission has been granted by a member of the senior leadership team in emergency circumstances.
- Staff should not use personally-owned devices, such as mobile phones or cameras, to take photos or videos of pupils and will only use work-provided equipment for this purpose.
- Staff may use their phones to access CPOMs verification applications as long as the device is password protected.

Digital images and video (see Use of cameras, and photographs policy 2019)

In this school:

- 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 (or annually);
- We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials/DVDs;
- Staff sign the school's Acceptable Use Policy and this includes a clause on the use of mobile phones/personal equipment for taking pictures of pupils;
- The school blocks/filter access to social networking sites unless there is a specific approved educational purpose;
- We do not store or display photographs that are over 5 years old. These are systematically deleted unless they are for archive purposes.