Saint Paulinus CE Primary School

Online Safety Policy

Principal and Designated Safeguarding Lead: Mrs Rhodes

Assistant Principal: Mrs Sukonik

Safeguarding Governor Lead: Mrs S Smith

Computing Lead: Mr B Hogan

Policy adopted: September 2023

Last Reviewed: August 2024

'As children of God at St Paulinus, we strive to create a happy, caring place where everybody is valued, respected and safe so we learn and grow to our very best.'

"Having gifts that differ according to the grace given to us, let us use them" (Romans 12,6)

NURTURE: Knowledge, Curiosity, Resilience, Respect, Spirituality, Creativity & Love

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 St Paulinus Church of England Primary School with respect to the use of Information Communication Technology (ICT) -based technologies
- safeguard and protect the children and staff of St Paulinus Church of England Primary School
- assist school staff working with children to work safely and responsibly with the internet and other 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
- draw awareness to online abuse such as cyberbullying which are cross referenced with other school policies and documentation
- ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken
- minimise the risk of misplaced or malicious allegations made against adults who work with students

Information Communication Technology (ICT) in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm young people with the skills to access life-long learning and employment.

At St Paulinus Church of England Primary School, we understand the responsibility to educate our pupils on e-Safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom. It is important to teach pupils about the underpinning knowledge and behaviours that can help pupils to navigate the online world safely and confidently, regardless of the device, platform or app.

This policy (for all staff, governors, visitors and pupils) includes both fixed and mobile internet; technologies provided by the school and technologies owned by pupils and staff, that may be brought onto school premises (such as laptops, mobile phones etc) or used at home for the purpose of remote teaching.

This policy covers all users of our school's ICT facilities, including governors, staff, pupils, volunteers, contractors and visitors. Breaches of this policy may be dealt with under our Staff Code of Conduct or Unacceptable Behaviour Policy.

Communication: How the policy will be communicated to staff/pupils/community:

- Policy to be posted on the school website/staffroom
- Acceptable Use Agreements discussed with pupils at the start of each year
- Acceptable Use Agreements to be issued to whole school community, usually on entry to the school
- Acceptable Use Agreements to be held in pupil and personnel files

Curriculum Context (DFE June 2019)

From September 2020, Relationships Education will be compulsory for all primary aged pupils, Relationships and Sex Education will be compulsory for all secondary aged pupils and Health Education will be compulsory in all state-funded schools in England.
Through these new subjects, pupils will be taught about online safety and harms. This will include being taught what positive, healthy and respectful online relationships look like, the effects of their online actions on others and knowing how to recognise and display respectful behaviour online. Throughout these subjects, teachers will address online safety and appropriate behaviour in an age-appropriate way that is relevant to their pupils' lives.
This will complement the computing curriculum, which covers the principles of online safety at all key stages, with progression in the content to reflect the different and escalating risks that pupils face. This includes how to use technology safely, responsibly, respectfully and securely, and where to go for help and support when they have concerns about content or contact on the internet or other online technologies.
There are also other curriculum subjects which include content relevant to teaching pupils how to use the internet safely. For example citizenship education covers media literacy - distinguishing fact from opinion as well as exploring freedom of speech and the role and

responsibility of the media in informing and shaping public opinion. It also supports teaching about the concept of democracy, freedom, rights, and responsibilities.

Relevant legislation and guidance

This policy refers to, and complies with, the following legislation and guidance:

- Data Protection Act 2018
- The General Data Protection Regulation
- Computer Misuse Act 1990
- Human Rights Act 1998
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Education Act 2011
- Freedom of Information Act 2000
- The Education and Inspections Act 2006
- Keeping children safe in education 2024
- Searching, screening and confiscation: advice for schools

Definitions

- **"ICT facilities":** includes all facilities, systems and services including but not limited to network infrastructure, desktop computers, laptops, tablets, phones, music players or hardware, software, websites, web applications or services, and any device system or service which may become available in the future which is provided as part of the ICT service
- **"Users":** anyone authorised by the school to use the ICT facilities, including governors, staff, pupils, volunteers, contractors and visitors
- **"Personal use":** any use or activity not directly related to the users' employment, study or purpose
- **"Authorised personnel":** employees authorised by the school to perform systems administration and/or monitoring of the ICT facilities
- **"Materials":** files and data created using the ICT facilities including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites, and blogs

Unacceptable Use

The following is considered unacceptable use of the school's ICT facilities by any member of the school community. Any breach of this policy may result in disciplinary or behaviour proceedings.

Unacceptable use of the school's ICT facilities includes:

- Using the school's ICT facilities to breach intellectual property rights or copyright
- Using the school's ICT facilities to bully or harass someone else, or to promote unlawful discrimination

- Breaching the school's policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate
- Activity which defames or disparages the school, or risks bringing the school into disrepute
- Sharing confidential information about the school, its pupils, or other members of the school community
- Connecting any device to the school's ICT network without approval from authorised personnel
- Setting up any software, applications or web services on the school's network without approval by authorised personnel, or creating or using any program, tool or item of software designed to interfere with the functioning of the ICT facilities, accounts or data
- Gaining, or attempting to gain, access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel
- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities
- Causing intentional damage to ICT facilities
- Removing, deleting or disposing of ICT equipment, systems, programs or information without permission by authorised personnel
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation
- Using inappropriate or offensive language
- Promoting a private business, unless that business is directly related to the school
- Using websites or mechanisms to bypass the school's filtering mechanisms

This is not an exhaustive list. The school reserves the right to amend this list at any time. The Principal will use professional judgment to determine whether any act or behaviour not on the list above is considered unacceptable
use of the school's ICT facilities.

Sanctions

Pupils and staff who engage in any of the unacceptable activity listed above may face disciplinary action in line with the school's policies on behaviour, staff code of conduct and/or unacceptable behaviour

Expected Conduct and Incident Management

In our school, all users:

- are responsible for using the school ICT systems in accordance with the relevant Acceptable Use Policy which they will be expected to sign before being given access to school systems (at KS1 it would be expected that parents/carers would sign on behalf of the pupils)

- need to understand the importance of misuse or access to inappropriate materials and are aware of the consequences
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- should understand the importance of adopting good e-Safety practice when using digital technologies out of school and realise that the school's e-Safety Policy covers their actions out of school, if related to their membership of the school
- will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking/use of images and on cyber-bullying

Staff
Key Responsibilities:

- be responsible for reading the school's e-Safety policy and using the school ICT systems accordingly, including the use of mobile phones, and hand held devices
- embed e-Safety issues in all aspects of the curriculum and other school activities
- supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant)
- to be aware of e-Safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices
- report any suspected misuse or problem to a Designated Safeguarding Lead
- maintain an awareness of current e-Safety issues and guidance e.g. through CPD
- model safe, responsible and professional behaviour in their own use of technology
- ensure that any digital communications with pupils should be on a professional level and only through school based systems, never through personal mechanisms, e.g. email, text, mobile phones etc

Students/Pupils
Key Responsibilities:

- should have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- read, understand, sign and adhere to the Student/Pupil Acceptable Use Policy (nb: at KS1 it would be expected that parents/carers would sign on behalf of the pupils)
- understand the importance of reporting abuse, misuse or access to inappropriate materials
- know what action to take if they or someone they know feels worried or vulnerable when using online technology
- know and understand school policy on the use of mobile phones, digital cameras and hand held devices
- know and understand school policy on the taking/use of images and on cyber-bullying
- understand the importance of adopting good e-Safety practice when using digital technologies out of school and realise that the school's eSafety Policy covers their actions out of school, if related to their membership of the school
- take responsibility for learning about the benefits and risks of using the internet and other technologies safely both in school and at home
- will be provided with an account linked to the school's virtual learning platform, which they can access from any device

Parents/Carers

- should provide consent for pupils to use the Internet, as well as other technologies, as part of the Acceptable Use Agreement form

- should know and understand what the 'rules of appropriate use' are and what sanctions result from misuse
- support the school in promoting e-Safety and endorse the Parents' Acceptable Use Agreement which includes the pupils' use of the internet and the school's use of photographic and video images
- read, understand and promote the school Pupil Acceptable Use Agreement with their children
- access the school website/on-line student resources and learning platforms/pupil records in accordance with the relevant school Acceptable Use Agreement
- consult with the school if they have any concerns about their children's use of technology

Parent/Carer Access to ICT facilities and materials

- Parents do not have access to the school's ICT facilities as a matter of course
- However, parents working for, or with, the school in an official capacity (for instance, as a volunteer or as a member of the PTA) may be granted an appropriate level of access, or be permitted to use the school's facilities at the Head of School's discretion
- Where parents are granted access in this way, they must abide by this policy as it applies to staff

Communicating with or about the school online

We believe it is important to model for pupils, and help them learn, how to communicate respectfully with, and about, others online. Parents play a vital role in helping model this behaviour for their children, especially when communicating with the school through our website and social media channels. We ask parents to sign the Parent/Carer Acceptable Use Agreement.

Parent Awareness and Training Our school:

We run a rolling programme of advice, guidance and training for parents, including:

- Introduction of the Acceptable Use Agreements to new parents, to ensure that principles of e-Safe behaviour are made clear
- Information leaflets; in school newsletters; on the school website
- suggestions for safe Internet use at home
- provision of information about national support sites for parents

Managing the ICT Infrastructure

Internet access, security (virus protection) and filtering

Our school:

- Has the educational filtered secure broadband connectivity through the London Grid for Learning (LGfL) and so connects to the 'private' National Education Network
- Uses the LGfL filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature, etc. All changes to the filtering policy is logged and only available to staff with the approved 'web filtering management' status Via the Atomwide helpdesk
- Uses Unified Sign-On (USO) user-level filtering where relevant, thereby closing down or opening up options appropriate to the age/stage of the students
- Ensures healthy network through use of Sophos anti-virus software (from LGfL) etc and network set-up so staff and pupils cannot download executable files

- Uses DfE, Local Authority (LA) or LGfL approved systems such as S2S, USO FX, secured email to send personal data over the Internet and uses encrypted devices or secure remote access where staff need to access personal level data off-site
- LGFL Blocks all chat rooms and social networking sites except those that are part of an educational network or approved Learning Platform
- Only unblocks other external social networking sites for specific purposes/Internet Literacy lessons
- Has blocked pupil access to music download or shopping sites – except those approved for educational purposes at a regional or national level, such as Audio Network
- Works in partnership with the LGfL to ensure any concerns about the system are communicated so that systems remain robust and protect students
- Is vigilant in its supervision of pupils' use at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas where older pupils have more flexible access
- Ensures all staff and students have signed an Acceptable Use Agreement form and understands that they must report any concerns
- Ensures pupils only publish within an appropriately secure environment: the school's learning environment/ the London LEARNING PLATFORM/ LGfL secure platforms such as J2Bloggy, etc
- Requires staff to preview websites before use (where not previously viewed or cached) and encourages use of the school's Learning Platform as a key way to direct students to age/subject appropriate websites; Plans the curriculum context for Internet use to match pupils' ability, using child-friendly search engines where more open Internet searching is required; eg yahoo for kids or ask for kids , Google Safe Search
- Never allows/is vigilant when conducting 'raw' image search with pupils eg Google image search
- Informs all users that Internet use is monitored
- Informs staff and students that that they must report any failure of the filtering systems directly to the (*system administrator/teacher/person responsible for URL filtering)*. Our system administrator(s) logs or escalates as appropriate to the technical service provider or Atomwide Helpdesk as necessary
- Makes clear all users know and understand what the 'rules of appropriate use' are and what sanctions result from misuse – through staff meetings and teaching programme
- Provides advice and information on reporting offensive materials, abuse/bullying etc available for pupils, staff and parents
- Immediately refers any material we suspect is illegal to the appropriate authorities (Police and the LA)

Network Management (User Access, Backup)

Our school:

- uses individual staff log-ins and pupil year group log-ins, audited log-ins for all users: the London USO system
- uses guest accounts occasionally for external or short-term visitors for temporary access to appropriate services; occasional guests do not have access to the public drive
- uses teacher 'remote' management control tools for controlling workstations/viewing users/setting-up applications and Internet websites, where useful
- has additional local network auditing software installed

- 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
- storage of all data within the school will conform to the UK data protection requirements. Pupils and Staff using mobile technology, where storage of data is online, will conform to the EU data protection directive where storage is hosted within the EU

To ensure the network is used safely, our school:

- ensures staff read and sign that they have understood the school's e-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/use the same username and password* for access to our school's network; staff individual log-ins and pupil year group log-in passwords changed annually
- staff access to the schools' management information system is controlled through a separate password for data security purposes; Sims system has restricted access for only the Office Staff and Senior Management only. Access granted by Sims team and agreed with the Office Manager and Head Teacher
- we provide pupils with a class network log-in username. From Year R they are also expected to use a class password
- we use the London Grid for Learning's USO system for username and passwords
- 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 as these have far less security restrictions and inappropriate use could damage files or the network
- 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 always log off when they have finished working or are leaving the computer unattended
- where a user finds a logged-on machine, we require them to always log-off and then log-on again as themselves (users needing access to secure data Target Tracker & Sims)
- requests that teachers and pupils do not switch the computers off during the day unless they are unlikely to be used again that day or have completely crashed. We request that they DO switch the computers off at the end of the day
- network users can download executable files/programmes but cannot run these programmes unless Teacher power user rights
- LGFL have blocked access to music/media download or shopping sites – except those approved for educational purposes
- makes clear that staff are responsible for ensuring that all equipment that goes home has the anti-virus and spyware software maintained up-to-date and the school provides them with a solution to do so
- makes clear that staff are responsible for ensuring that any computer or laptop loaned to them by the school is used solely to support their professional responsibilities and that they notify the school of any "significant personal use" as defined by HM Revenue & Customs
- *makes clear that staff accessing LA systems do so in accordance with any Corporate policies e.g. Borough email or Intranet; finance system, Personnel system etc;*
- maintains equipment to ensure Health and Safety is followed eg projector filters cleaned by site manager/TA; equipment installed and checked by approved Suppliers/LA electrical engineers
- has integrated curriculum and administration networks, but access to the Management Information System is set-up so as to ensure staff users can only

access modules related to their role eg teachers access report writing module; SEN coordinator - SEN data as setup by Atomwide helpdesk
- ensures that access to the school's network resources from remote locations by staff is restricted and access is only through school/LA approved systems *eg teachers access their area/a staff shared area for planning documentation via a VPN solution / RAv3 system;* (Rav3 access for administrator and Head Teachers only)
- does not allow any outside Agencies to access our network remotely except where there is a clear professional need and then access is restricted and is only through approved systems eg technical support or MIS Support, our Education Welfare Officers accessing attendance data on specific children, parents using a secure portal to access information on their child
- provides pupils and staff with access to content and resources through the approved LGFL Learning Platform which staff and pupils access using their username and password (their USO username and password)
- makes clear responsibilities for the daily back up of MIS and finance systems and other important files
- has a clear disaster recovery system in place for critical data that includes a secure, remote back-up of critical data, that complies with external Audit's requirements;
- uses the DfE secure s2s website for all CTF files sent to other schools as set up by the Sims team
- 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)
- follows ISP advice on Local Area and Wide Area security matters and firewalls and routers have been configured to prevent unauthorised use of our network;
- our wireless network has been secured to industry standard Enterprise security level /appropriate standards suitable for educational use
- all computer equipment is installed professionally and meets health and safety standards

- projectors are maintained so that the quality of presentation remains high
- reviews the school ICT systems regularly with regard to health and safety and security
- Use SENSO to monitor computer usage.

E-Safety and the PREVENT strategy

Our policy and practice ensures that:

- Children are safe from terrorist and extremist material when accessing the internet in school, including by establishing appropriate levels of filtering (through appropriate school level and/or external (LGfL) filtering
- We ensure pupils cannot access dangerous content, or be contacted online by extremist groups
- General internet safety is embedded in our school's computing curriculum
- Every teacher is aware of the risks posed by the online activity of extremist and terrorist groups

Passwords Policy

- This school makes it clear that staff and pupils must always keep their password private. They **must not share it** with others and must not leave it where others can find

- All staff have their own unique username and private passwords to access school systems. **Staff are responsible for keeping their password private**
- We require staff to use a STRONG password for access into our MIS system

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
- does not publish personal e-mail addresses of pupils or staff on the school website. We use anonymous or group e-mail addresses, eg info@schoolname.la.sch.uk / head@schoolname.la.sch.uk / or class e-mail addresses (with one or more staff having access to an aliased/shared mailbox for a class) for communication with the wider public
- 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
- reports messages relating to or in support of illegal activities to the relevant Authority and if necessary to the Police
- knows that spam, phishing and virus attachments can make emails dangerous. 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 e-mail filtering for viruses, Trojans, pornography, phishing and inappropriate language. Finally, and in support of these, LGfL WebScreen2 filtering monitors and protects our internet access to the World Wide Web

Pupils:

- Pupils are introduced to email as part of the Computing Scheme of Work
- Pupils sign the school Agreement Form to say they have read and understood the e-safety rules, including e-mail

Staff:

- Staff can only use the LA, paulinus.co.uk and LGfL e-mail systems on the school system
- Staff use a 'closed' LA e-mail system which is used for LA communications and some 'LA approved' transfers of information
- Never use e-mail to transfer staff or pupil personal data. We use secure, LA/DfE approved systems. These include: S2S (for school to school transfer); Collect; USO-FX*, Atomwide*
- Staff know that e-mail sent to an external organisation must be written carefully, (and may require authorisation), in the same way as a letter written on school headed paper. That it should follow the school 'house-style'
- The sending of multiple or large attachments should be limited, and may also be restricted by the provider of the service being used
- The sending of chain letters is not permitted
- Embedding adverts is not allowed
- All staff sign our E-Safety and Acceptable Use Agreement Form to say they have read and understood the e-safety rules, including e-mail and we explain how any inappropriate use will be dealt with

Social Networking

- Teachers are instructed not to run social network spaces for student use on a personal basis or to open up their own spaces to their students, but to use the schools' preferred system for such communications
- School staff will ensure that in private use
    - No reference should be made in social media to students/pupils, parents/carers or school staff
    - They do not engage in online discussion on personal matters relating to members of the school community
    - Personal opinions should not be attributed to the *school/academy* or local authority
    - Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information

Equipment and Digital Content

Staff and Student Use of Personal Devices:

- Mobile phones or iPads brought into school are entirely at the staff member, student's & parents' or visitor's own risk. The School accepts no responsibility for the loss, theft or damage of any phone or handheld device brought into school
- Student mobile phones which are brought into school must be turned off (not placed on silent) and stored in the school office until collection at the end of the day
- The recording, taking and sharing of images, video and audio on any mobile phone or personal iPad is to be avoided; except where it has been explicitly agreed otherwise by the Principal. Such authorised use is to be monitored and recorded. All use is to be open to scrutiny and the Principal is to be able to withdraw or restrict authorisation for use at any time if it is to be deemed necessary
- The School reserves the right to search the content of any mobile or handheld device on the school premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying. Staff mobiles or hand held devices may be searched at any time as part of routine monitoring
- Where parents or students need to contact each other during the school day, they should do so only through the School's telephone. Staff may use their phones during break times
- Mobile phones and personally-owned devices will not be used in any way during lessons or formal school time. They should be switched off or silent at all times
- In an emergency for contacting students or parents a staff member should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes
- Staff may not use the school's ICT facilities to store personal non-work-related information or materials (such as music, videos, or photos)
- Staff should be aware that use of the school's ICT facilities for personal use may put personal communications within the scope of the school's ICT monitoring activities)
- Staff should be aware that personal use of ICT (even when not using school ICT facilities) can impact on their employment by, for instance putting personal details in the public domain, where pupils and parents could see them

- Staff should take care to follow the school's guidelines on social media and use of email to protect themselves online and avoid compromising their professional integrity
- If a member of staff breaches the school policy then disciplinary action may be taken
- Under the Education Act 2011, and in line with the Department for Education's guidance on searching, screening and confiscation, the school has the right to search pupils' phones, computers or other devices for pornographic images or any other data or items banned under school rules or legislation

Digital Images and Video
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
- We do include the full names of pupils in the credits of any published school produced video materials/DVDs
- Staff sign the school's Acceptable Use Policy and this includes a clause on the use of mobile phones/personal equipment for taking pictures of pupils
- If specific pupil photos (not group photos) are used on the school website, in the prospectus or in other high profile publications the school will obtain individual parental or pupil permission for its long-term use
- The school blocks/filters access to social networking sites or news groups unless there is a specific approved educational purpose
- Pupils are taught about how images can be manipulated in their e-Safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children as part of their ICT scheme of work
- Pupils are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information
- Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identify of others and their location, such as house number, street name or school. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse

School Website

- The Principal takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained
- Uploading of information is restricted to our website authorisers
- The school website complies with the statutory DfE guidelines for publications
- 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
- The point of contact on the website is the school address, telephone number and we use a general e-mail contact address, admin@st-paulinus.bexley.sch.uk. Home information or individual e-mail identities will not be published
- 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
- We do not use embedded geo-data in respect of stored images

- We expect teachers using school approved blogs or wikis to password protect them and run from the school website

Video Conferencing

The school has followed recommendations issued by the National Cyber Security Centre (NCSC) (April 2020), including the NCSC's Cloud Security Guidance (November 2018) when choosing a platform to host video conferencing with staff and pupils. This guidance should also be read in conjunction with *Zoom Video Communications Cloud Security Principles (NCSC UK)* (September 2020).

Guidance Followed by Staff Organising Meetings:

- Being able to control who can join (or initiate) meetings will help protect the confidentiality of the discussions, and prevent unwanted interruptions. Participants join meetings arranged in advance by clicking on a link, or by entering a unique code
- Staff use single sign-on, integrating the video conferencing service with our existing corporate identity. This means that the service inherits the same identity protections as our other corporate services. It significantly improves the user experience by reducing the number of times that authentication is required
- Users should be required to enter a passcode
- Unauthenticated users should be held in a waiting area (often referred to as 'the lobby'), and only be admitted into the meeting once their identity has been verified by a trusted participant

During the video conference, meeting organisers take responsibility for:

- verifying the identity of all participants on the call
- appropriately approving participants being held in the lobby
- removing participants that have not been successfully identified

Safer use of Zoom by staff:

- The Zoom Meeting ID is not displayed on the title toolbar.
- The Waiting Room feature is on by default
- Meeting passwords are on by default.
- Account admins and hosts can disable the ability for participants to rename themselves (for every meeting)
- Staff use a new meeting room each time (ie. don't use the personal meeting ID)
- Attendees are not allowed to join before the host
- Screen sharing is not available to pupils
- A 'waiting room' is set up for every meeting
- Meeting details are only shared on platforms that are part of our existing corporate identity (i.e. parentmail and Google Classroom).
- Teachers can restrict the in-class chat so students cannot privately message other students. Sign in to the **Zoom** web portal. In the navigation menu, click Settings. Navigate to **Chat** option under In Meeting (Basic). Click the **Chat** and **Private Chat** toggles to disable in-meeting **chat**.

Remote access

We allow staff to access the school's ICT facilities and materials remotely.

Staff accessing the school's ICT facilities and materials remotely must abide by the same rules as those accessing the facilities and materials on-site. Staff must be particularly vigilant if they use the school's ICT facilities outside the school and take such precautions against importing viruses or compromising system security.

Our ICT facilities contain information which is confidential and/or subject to data protection legislation. Such information must be treated with extreme care and in accordance with our data protection policy.

Asset Disposal

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.
All redundant equipment will be disposed of through an authorised agency. This will include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.
All redundant equipment that may have held personal data will have the storage media forensically wiped. Alternatively, if the storage media has failed, it will be physically destroyed. The school will only use authorised companies who will supply a written guarantee that this will happen.
Disposal of any equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2006 and/or The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007. Further information can be found on the Environment Agency website.