City of London School
IT and Acceptable Use Policy

Policy reviewed by:	Adam Zivanic
Date last reviewed:	August 2025
Approved by:	Board of Governors
Date approved:	3 December 2025

This policy should be read in conjunction with:

- Safeguarding and Child Protection Policy
- Behaviour Policy
- Anti-Bullying Policy
- Teachers' Standards
- City of London Corporation Acceptable Use of IT Policy
- City of London Corporation Data Protection Policy
- City of London Corporation Employee Code of Conduct
- City of London Corporation Disciplinary Policy
- City of London Corporation Social Media policy

Contents

1. Introduction and aims 3
2. Relevant legislation and guidance 3
3. Definitions 4
4. Acceptable use 4
5. Staff (including governors, volunteers, and contractors) 6
6. Pupils 10
7. Parents/carers 12
8. Visitors 13
9. Data security 14
10. Protection from cyber attacks 16
11. Internet access 17
12. eSafety 18
13. Monitoring and review 19
Appendix 1: Cybersecurity Strategy 20
Appendix 2: Glossary of cyber security terminology 29
Appendix 3: Roles and responsibilities for eSafety 32
Appendix 4: eSafety on the curriculum 36

1. Introduction and aims

Information and communications technology (ICT) is an integral part of the way our school operates, and is a critical resource for pupils, staff, governors, volunteers and visitors. It supports teaching and learning, and the pastoral and administrative functions of the school.

However, the ICT resources and facilities our school uses could also pose risks to data protection, online safety and safeguarding.

This policy aims to:

- Set guidelines and rules on the use of school ICT resources for staff, pupils, parents/carers and governors
- Establish clear expectations for the way all members of the school community engage with each other online
- Support the school's policies on data protection, data retention and data breaches
- Prevent disruption that could occur to the school through the misuse, or attempted misuse, of ICT systems
- Ensure that the school has robust processes in place to ensure online safety of pupils, staff, volunteers and governors.
- Establish an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology and allow our pupils to foster a sense of independence and resilience in the digital age whilst emphasising the opportunities that technology can provide.
- To ensure that online safety is understood to be vital to safeguarding as a whole and be treated with equal focus. It is not a separate issue.

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 Behaviour Policy or Disciplinary Policy.

2. Relevant legislation and guidance

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

- Data Protection Act 2018
- The UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020
- Computer Misuse Act 1990
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

- Education Act 2011
- Freedom of Information Act 2000
- Education and Inspections Act 2006
- Keeping Children Safe in Education 2025
- Searching, screening and confiscation: advice for schools 2022
- National Cyber Security Centre (NCSC): Cyber Security for Schools
- UK Council for Internet Safety (et al.) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Meeting digital and technology standards in schools and colleges

3. Definitions

- **ICT facilities:** 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 that may become available in the future which is provided as part of the school's ICT service
- **Users:** anyone authorised by the school to use the school's 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 agreed by an authorised user
- **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 school's ICT facilities including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites and blogs

See appendix 2 for a glossary of cyber security terminology.

4. Acceptable use

The following is considered unacceptable use of the school's ICT facilities. Any breach of this policy may result in disciplinary (staff) or behaviour (pupils) proceedings (see section 5.2 below).

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

- Online gambling, inappropriate advertising, phishing and/or financial scams
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate or harmful
- Consensual and non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams
- 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 programme, tool or item of software designed to interfere with the functioning of the school's 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 the school's ICT facilities
- Removing, deleting or disposing of the school's ICT equipment, systems, programmes or information without permission from authorised personnel
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not permitted by authorised personnel 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 or monitoring mechanisms
- Engaging in content or conduct that is radicalised, extremist, racist, antisemitic or discriminatory in any other way
- Saving personal files (irrespective of size) on school's OneDrive/ SharePoint spaces

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

4.1 Exceptions from unacceptable use

Wherever possible, staff, pupils and visitors should comply with the acceptable use and seek help from IT services to find a way to work in a compliant way. No exceptions should be granted until all the suitable alternatives have been explored.

Where the use of school ICT facilities (on the school premises and/or remotely) is required for a purpose that would otherwise be considered an unacceptable use, exemptions to the policy may be granted at the Head's discretion. The Head might delegate such decision to the Senior Deputy Head/ Director of Digital Strategy.

4.2 Sanctions

Pupils and staff who engage in any of the unacceptable activities listed above may face disciplinary action in line with the school's Behaviour Policy and CoL Teachers Guide (section E).

4.3 Printing

The use of school printing services must be in accordance with the following:

- Consideration on the environmental impact and cost implications of printing
- Defaults are black & white and duplex (double sided printing) which can be overridden at time of print/copy
- Print counts are recorded and used for internal reporting and billing from our print supplier
- Limited personal printing is permitted

5. Staff (including governors, volunteers, and contractors)

5.1 Access to school ICT facilities and materials

The school's Director of Digital Strategy/ IT Systems Managers/ Systems Engineers manage access to the school's ICT facilities and materials for school staff. That includes, but is not limited to:

- Computers, tablets, mobile phones and other devices
- Access permissions for certain programmes or files

Staff will be provided with unique login/account information and passwords that they must use when accessing the school's ICT facilities.

Staff who have access to files that they are not authorised to view or edit, or who need their access permissions updated or changed, should contact the IT services and, if appropriate, report potential data breach.

Use of phones and email

The school provides each member of staff with an email address.

This email account should be used for work purposes only. Staff should enable multi-factor authentication on their email account(s). School will give guidance on the most appropriate method of authentication.

All work-related business should be conducted using the email address the school has provided.

Staff members should not send unnecessary messages to a large number of people. This is sometimes called spamming. Dealing with these messages wastes time and system resources. Distribution groups should only be used for official school business and not for personal messages.

Staff must not share their personal email addresses with parents/carers and pupils, and must not send any work-related materials using their personal email account.

Staff must take care with the content of all email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract.

Email messages are required to be disclosed in legal proceedings or in response to requests from individuals under the Data Protection Act 2018 in the same way as paper documents. Deletion from a user's inbox does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable.

Staff must take extra care when sending sensitive or confidential information by email. Any attachments containing sensitive or confidential information should be encrypted so that the information is only accessible by the intended recipient.

If staff receive an email in error, the sender should be informed and the email deleted. If the email contains sensitive or confidential information, the user must not make use of that information or disclose that information and must report this to the Data Protection Officer.

Staff who email groups of parents must avoid exposing all of the email addresses to all of the recipients. When sending out a group email to parents, users must place their own email address in the "To" field, and the email addresses of the intended recipients in the "bcc" field.

If staff send an email in error that contains the personal information of another person, they must inform the Data Protection Officer immediately and follow our data breach procedure.

Staff must not give their personal phone number(s) to parents/carers or pupils. Staff must use phones provided by the school to conduct all work-related business. If, in exceptional circumstances, staff have to use personal mobile phones, calls should be made using withheld number option.

School phones must not be used for personal matters.

Staff who are provided with mobile phones as equipment for their role must abide by the same rules for ICT acceptable use as set out in section 4.

5.2 Personal use

Staff are permitted to occasionally use school ICT facilities for personal use, subject to certain conditions set out below. This permission must not be overused or abused. The Head/ Director of Digital Strategy/ Senior Deputy Head may withdraw or restrict this permission at any time and at their discretion.

Personal use is permitted provided that such use:

- Does not take place during teaching time/ supervised activities
- Does not constitute 'unacceptable use', as defined in section 4
- Takes place when no pupils are present

- Does not interfere with their jobs, or prevent other staff or pupils from using the facilities for work or educational 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). This extends to, but is not limited to Google Drives, SharePoint, OneDrive and iCloud accounts linked to school accounts.

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 (see section 5.5). Where breaches of this policy are found, disciplinary action may be taken.

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/carers could see them.

Staff should take care to follow the school's guidelines on use of social media and use of email (see section 6.1.1 and Appendix 2 of the City of London Acceptable Use of IT Policy) to protect themselves online and avoid compromising their professional integrity.

5.3 Remote access

We allow staff to access the school's ICT facilities and materials remotely using Microsoft 365 services. We discourage use of external storage devices for carrying work-related files outside of the school and encourage all staff to familiarise themselves with best practices related to working with data on multiple devices.

Any use of personal devices for School purposes, and any removal of personal data or confidential information from school systems (by any means, including email, printing, file transfer, or cloud-based storage) must be registered with and approved by a member of school staff responsible for the data in question.

Some staff will need access to different City of London resources and, to access these, should dial in using a virtual private network (VPN). Such access should be requested by line managers during the onboarding process from IT services. Should VPN access be required after a member of staff has commenced their employment, they should make the request to IT services and copy in their line manager for confirmation of the need for VPN access.

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 must take all the necessary precautions to avoid compromising school's IT systems.

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. Staff should not be accessing such information in public spaces where the information might be seen/ accessed by others. Devices on which such information is accessed, including all school devices, should never be left unlocked when unsupervised.

5.4 Monitoring and filtering of the school network and use of ICT facilities

To safeguard and promote the welfare of children and provide them with a safe environment to learn, the school reserves the right to filter and monitor the use of its ICT facilities and network. This includes, but is not limited to, the filtering and monitoring of:

- Internet sites visited
- Bandwidth usage
- Email accounts
- Telephone calls
- User activity/access logs
- Any other electronic communications

Only authorised ICT personnel and the Director of Digital Strategy/ the Head/ Senior Deputy Head may filter, inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law.

The school monitors ICT use in order to:

- Obtain information related to school business
- Investigate compliance with school policies, procedures and standards
- Ensure effective school and ICT operation
- Conduct training or quality control exercises
- Prevent or detect crime
- Comply with a subject access request, Freedom of Information Act request, or any other legal obligation

Our Board of Governors is responsible for making sure that:

- The school meets the DfE's filtering and monitoring standards
- Appropriate filtering and monitoring systems are in place
- Staff are aware of those systems and trained in their related roles and responsibilities
- For the leadership team and relevant staff, this will include how to manage the processes and systems effectively and how to escalate concerns
- It regularly reviews the effectiveness of the school's monitoring and filtering systems

The school's designated safeguarding lead (DSL) will take lead responsibility for understanding the filtering and monitoring systems and processes in place.

Where appropriate, staff may raise concerns about monitored activity with the school's DSL and the Director of Digital Strategy, as appropriate.

6. Pupils

6.1 Access to ICT facilities

Following ICT facilities are available to pupils:

- Sets of laptop computers to be used for teaching of the groups without personal devices – OG and First Form (must be signed out by the teacher and returned at the earliest opportunity)
- Computer rooms – 306 and W3 – to be used with teacher supervision
- Laptops, which are issued to all pupils in Second to Fifth Form
- Pupils are provided with personal Microsoft 365 accounts that they can use for accessing learning materials and communication

6.2 Search and deletion

Under the Education Act 2011, the Head, and any member of staff authorised to do so by the Head, can search pupils and confiscate their mobile phones, computers or other devices that the authorised staff member has reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried out and/or
- Is evidence in relation to an offence

This includes, but is not limited to:

- Pornography
- Abusive messages, images or videos
- Indecent images of children
- Evidence of suspected criminal behaviour (such as threats of violence or assault)

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation (available by searching www.gov.uk)
- The UK Council for Internet Safety (UKCIS) et al.'s guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people (available by searching www.gov.uk)
- The School's Behaviour policy
- The School's Pupil Searches and Confiscation of Pupils' Belongings Policy

6.3 Unacceptable use of ICT and the internet outside of school

The school will sanction pupils, in line with the Behaviour Policy, if a pupil engages in any of the following **at any time** (even if they are not on school premises):

- Using ICT or the internet to breach intellectual property rights or copyright
- Using ICT or the internet to bully or harass someone else, or to promote unlawful discrimination
- Breaching the school's policies or procedures
- Any illegal conduct, or making 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
- Consensual or non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams (also known as sexting or youth produced sexual imagery)
- Activity which defames or disparages the school, or risks bringing the school into disrepute
- Sharing confidential information about the school, other pupils, or other members of the school community
- 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 the school's ICT facilities or materials
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user and/or those they share it with are not supposed to have access, or without authorisation
- Using inappropriate or offensive language

6.4 Unacceptable use of School-issued laptops

Pupils are expected to look after the devices issued to them and to regularly check and install the updates available.

The school will sanction pupils, in line with the Behaviour Policy, if a pupil engages in any of the following **at any time** (even if they are not on school premises):

- Intentionally damaging own or other pupils' laptops through inappropriate use
- Not reporting damage to laptops (intentional or accidental) to IT services for timely repair
- Causing damage to the equipment by leaving it in inappropriate places when not in use (e.g. not storing laptops in lockers)
- Gaining or trying to gain access to other pupils' laptops

- Installing software that has not been made available by IT services on Company Portal or authorised by teacher and installed by IT admins
- Using apps or cloud services of any kind to circumnavigate School's and general filtering and monitoring services (including, but not limited to VPNs, proxy websites etc.)
- Using browsers, such as, but not limited to Opera GX, in order to circumnavigate School's filtering and monitoring policies

6.5 Social Networking sites

The majority of social media sites and apps require users to be at least 13 years of age to access and use their services. This includes Facebook, Snapchat, X, Instagram, TikTok and WhatsApp. Whilst there is no age restriction for watching videos on YouTube, users need to be 13 or older to have their own YouTube account (enabling them to subscribe to other channels, like videos, post comments, share their own content and flag inappropriate content).

We expect all pupils to adhere to the age restrictions put in place by social media services.

All users of the school network (whether using school computers, personal laptops or any other portable electronic device that can connect to the school network) are not permitted to do the following:

- use social media, chat rooms or internet forums, other than as part of a lesson supervised by a member of staff
- violate copyright laws

7. Parents/carers

7.1 Access to ICT facilities and materials

Parents/carers do not have access to the school's ICT facilities as a matter of course.

However, parents/carers 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 headteacher's discretion.

Where parents/carers are granted access in this way, they must abide by this policy as it applies to staff.

7.2 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/carers 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.

8. Visitors

8.1 WiFi

To use visitor WiFi, visitors connect to CLS-Guest-WiFi. They will need to register to use this service and they will need to provide reception@cityoflondonschool.org.uk as their sponsor for the approval.

8.2 Monitoring

By accessing and using the School's guest Wi-Fi and internet services, visitors agree to abide by all applicable UK laws and School policies. All activity conducted over the School network may be monitored and logged in accordance with the Department for Education's Filtering and Monitoring Standards (October 2024). Visitors' use of this service is subject to compliance with the following legislation:

- UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018, as amended by the Data (Use and Access) Act 2025
- Computer Misuse Act 1990
- Copyright, Designs and Patents Act 1988 and relevant amendments, including the Copyright and Trade Marks (Offences and Enforcement) Act 2002

Filtering and monitoring systems are in place to safeguard users and ensure compliance with legal and safeguarding obligations. These systems may include real-time alerts and activity logs, and apply to all devices connected to the network, including BYOD and guest devices

If visitors do not agree to these terms, they should refrain from using the School's Wi-Fi services.

8.3 Unacceptable use

Visitors must not:

- access network services in such a way as to deny reasonable access to the network for other users, including, for example, excessive use of network bandwidth.
- download any material that is in breach of copyright. The school accepts no responsibility for any breaches that may occur.
- deliberately visit, view or download any material from any website containing pornographic, abusive, racist, violent or illegal material, nor material that is offensive in any way whatsoever or inappropriate in the context of teaching and learning and/or a school environment.
- upload or make available to others any material that is offensive, obscene, indecent, or which infringes the copyright of another person (e.g. images, MP3/4 and other audio or video files).
- use the Internet to harass, cause annoyance, inconvenience or anxiety to others.

- access, or attempt to gain access to, computer systems, data or resources to which you are not authorised.

9. Data security

The school is responsible for making sure it has the appropriate level of security protection and procedures in place to safeguard its systems, staff and learners. It therefore takes steps to protect the security of its computing resources, data and user accounts. The effectiveness of these procedures is reviewed periodically to keep up with evolving cyber crime technologies.

Staff, pupils, parents/carers and others who use the school's ICT facilities should use safe computing practices at all times. We aim to meet the cyber security standards recommended by the Department for Education's guidance on digital and technology standards in schools and colleges, including the use of:

- Firewalls
- Security features
- User authentication and multi-factor authentication
- Anti-malware software

9.1 Passwords

All users of the school's ICT facilities should set strong passwords for their accounts and keep these passwords secure.

Users are responsible for the security of their passwords and accounts, and for setting permissions for accounts and files they control.

Members of staff or pupils who disclose account or password information may face disciplinary action. Parents, visitors or volunteers who disclose account or password information may have their access rights revoked. Any user (staff or pupil) who suspects their account might have been compromised must report this to IT services immediately.

9.2 Software updates, firewalls and anti-virus software

All of the school's ICT devices that support software updates, security updates and anti-virus products will have these installed, and be configured to perform such updates regularly or automatically.

Users must not circumvent or make any attempt to circumvent the administrative, physical and technical safeguards we implement and maintain to protect personal data and the school's ICT facilities. Staff will be given training on how to run updates on their school laptops and are expected to run optional updates regularly or to seek help from IT services with running these.

Any personal devices using the school's network must all be configured in this way.

9.3 Access to facilities and materials

All users of the school's ICT facilities will have clearly defined access rights to school systems, files and devices.

These access rights are managed by Director of Digital Strategy, IT Systems Managers and Data Manger.

Users should not access, or attempt to access, systems, files or devices to which they have not been granted access. If access is provided in error, or if something a user should not have access to is shared with them, they should alert IT Services and Data Protection Officer immediately.

Users should always log out of systems and lock their equipment when they are not in use to avoid any unauthorised access. Equipment and systems should always be logged out of and shut down completely at the end of each working day. If equipment is left unlocked and unsupervised Director of Digital Strategy/ IT Systems Manager reserve the right to remove user's access and refer the breach of this policy to Senior Deputy Head for consideration.

9.4 Encryption

The school makes sure that its devices and systems have an appropriate level of encryption.

School staff may only use personal devices (including computers and USB drives) to access school data, work remotely, or take personal data (such as pupil information) out of school if they have been specifically authorised to do so by the Headmistress/ Senior Deputy Head.

Use of such personal devices will only be authorised if the devices have appropriate levels of security and encryption.

9.5 Retention of digital data

In line with the City of London Acceptable use of IT Policy and School Data Retention Policy, staff and pupils must be aware that:

- Emails sent or received on school systems may be routinely deleted or archived after a reasonable period, as outlined in the school's Email Retention Policy.
- On leaving the school community, email accounts will be closed and the contents deleted/archived after a reasonable period (normally no longer than one year), as outlined in the school's email deletion policy.
- In order that no important information should ever be lost as a result of the school's email deletion policy, it is the responsibility of each account user to ensure that important information (or indeed any personal information that they wish to keep, in line with school policy on personal use) is retained in the right place or, where applicable, provided to the right colleague.
- Important information that is necessary to be kept should be held in the relevant school personnel or pupil records, not kept in personal folders, archives or inboxes.

10. Protection from cyber attacks

Please see the glossary (appendix 2) to help you understand cyber security terminology.

“Cyber Security” describes the approach within which accountability, standards, policies and procedures are developed, implemented and maintained to ensure that all types of information used in the school are sourced, held and used appropriately, securely and legally, utilising technology and connectivity to its full advantage to operate within cyberspace.

Detailed background on Cybersecurity Strategy can be found in the appendix 1.

The school will:

- Work with governors and the IT department to make sure cyber security is given the time and resources it needs to make the school secure
- Provide relevant training for staff (and include this training in any induction for new starters, if they join outside of the school’s annual training window) on the basics of cyber security, including how to:
    - Check the sender address in an email
    - Respond to a request for bank details, personal information or login details
    - Verify requests for payments or changes to information
- Make sure staff are aware of its procedures for reporting and responding to cyber security incidents
- Investigate whether our IT software needs updating or replacing to be more secure
- Not engage in ransom requests from ransomware attacks, as this would not guarantee recovery of data
- Put controls in place that are:
    - **Proportionate**
    - **Multi-layered**: everyone will be clear on what to look out for to keep our systems safe
    - **Up to date:** with a system in place to monitor when the school needs to update its software
    - **Regularly reviewed and tested**: to make sure the systems are as effective and secure as they can be
- Back up critical data and store these backups on cloud-based back up systems. The school will use cloud-to-cloud back-up service for personal and departmental files and cloud-based MIS for critical data.
- Delegate specific responsibility for maintaining the security of our management information system (MIS) to It Systems Manager and Data Manger
- Make sure staff:
    - Have access to personal devices through which they can access school files and data

    - Dial into our CoL network using a virtual private network (VPN) when working from home
    - Enable multi-factor authentication where they can, on things like school email accounts
    - Store passwords securely using a password manager
    - Use SSO wherever possible
- Make sure line managers conduct regular access reviews to make sure each user in the school has the right level of permissions and admin rights and report any inconsistencies to IT services
- Have a firewall in place that is switched on
- Develop, review and test an incident response plan with the IT department including, for example, how the school will communicate with everyone if communications go down, who will be contacted and when, and who will notify Action Fraud of the incident.

11. Internet access

The school's wireless internet connection is secure.

School has:

- Filtering mechanisms in place for staff and pupil networks
- Separate networks for staff, pupils and visitors

Filtering systems are not foolproof. Any member of staff or pupil is responsible for reporting access to inappropriate web material to IT services immediately. Staff should also alert the Director of Digital Strategy.

11.1 Pupils

Pupils have:

- Access to filtered WiFi network throughout the school
- Filtering and monitoring of the network is done through Senso.cloud and Lightspeed
- Any issues with accessing the network should be reported to IT services

11.2 Parents/carers and visitors

Parents/carers and visitors to the school will not be permitted to use the school's WiFi unless specific authorisation is granted by the IT service through the specific visitors WiFi network.

Staff must not give the WiFi password to anyone who is not authorised to have it. Doing so could result in disciplinary action.

12. eSafety

12.1 Categories of risk

Our approach to online safety is based on addressing the following categories of risk in line with the Keeping Children Safe in Education 2024:

- Content – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.
- Contact – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
- Conduct – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- Commerce – risks such as online gambling, inappropriate advertising, phishing and/or financial scam

12.2 Roles and responsibilities

All members of the school community are responsible for eSafety, as this is an integral part of our approach to safeguarding our pupils. Roles and responsibilities of specific groups are covered in the appendix 5.

12.3 Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum. Outline of this provision is covered in the Appendix 6.

12.4 Educating parents about online safety

The school will raise parents' awareness of internet safety and cyber security in information evenings, letters or other communications home, and in information via our website, Parent Portal and newsletter.

This policy will also be available to parents.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the Director of Digital Strategy or Deputy Head Pastoral/ DSL. Concerns or queries about this policy can be raised with any member of staff or the headmistress. Any concern about cyber security should be passed to the IT team/ Director of Digital Strategy.

12.5 Staff training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

All staff read Keeping Children Safe in Education annually and through discussions and completion of any quizzes the school deem necessary, demonstrate an understanding of their obligations and training.

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element
- Children can abuse their peers online through:
    - Abusive, harassing, and misogynistic messages
    - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
    - Sharing of abusive images and pornography or video/audio, to those who don't want to receive such content

Training will also help staff:

- develop better awareness to assist in spotting the signs and symptoms of online abuse
- develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh the risks up
- develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term.

The DSL and DDSLs will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

Phishing attack simulations

- IT team will run phishing attack simulations with the aim of identifying the most vulnerable staff and pupils and providing the appropriate training for those

13. Monitoring and review

The Head and Director of Digital Strategy/ IT Systems Manager monitor the implementation of this policy, including ensuring it is updated to reflect the needs and circumstances of the school.

This policy will be reviewed every two years.

Appendix 1: Cybersecurity Strategy

The growth of the internet as a commercial and social tool has had a dramatic effect on society. Cyberspace 'Cloud' is now a major marketplace for many organisations in the private and public education sectors, and is a key mechanism for engagement with pupils, parents and prospective parents. However, the increased reliance on the internet has exposed organisations to a host of new risks, presenting security challenges that did not exist in the pre-internet age. It is now possible for very damaging attacks to be mounted against an organisation from thousands of miles away, the aims of which may be to steal data, disrupt services or cause reputational damage. For this reason, cyber-security is high on the agenda within the school.

A National Cyber Strategy was published in 2016, followed by the formation of the Office of Cyber-Security and Information Assurance, which works with other bodies such as the Home Office, Ministry of Defence, GCHQ, CESG, CPNI and BIS to determine priorities for managing security in cyberspace. This has been underpinned within the City of London Corporation by 'Project Griffin' and an overall review of cyber security policies and practices across its organisational departments.

This strategy is informed by the work of these bodies, by industry best practice, and by engagement with security experts from the public and private sectors. It presents a mechanism for implementing proportionate technical and procedural security controls, designed to provide assurance that the school's information assets will be protected from cyber-security threats, whilst fully acknowledging the requirement for the organisation to be agile and responsive.

The increasing volume and sophistication of cyber-security threats, especially targeting public organisations and institutions, demands that the school takes a structured, strategic approach to securing our information systems, in order to provide the best possible protection to our data, and assurance to our pupils, parents and prospective parents.

This strategy defines the technical and procedural framework that will provide the best possible security for the school's data:

- it outlines a risk-based approach, designing security measures that are appropriate in the context of the school's educational objectives, responsibilities and budget.
- it ensures that information security is a business-enabler by providing the framework for the school to use its information assets in the safest possible way, in order to gain the maximum business benefit.
- it outlines measures to ensure that the responsibility for cyber-security is understood by all staff.
- it provides a roadmap to achieving compliance within national guidance on security and information assurance.

Strategic principles

This Cyber-Security Strategy is based on a number of underlying principles, designed to ensure that the protective measures are thorough, proportionate and cost-effective. These principles are brought together through information security controls defined within the strategic objectives and though the key principles of people, process and technology all working together in order to achieve our strategic objectives:

- **People:** ensuring staff are equipped to handle information respectfully and safely
- **Process:** proactively preventing data security breaches
- **Technology:** providing secure and up-to-date technology

Principle 1: Defence in depth

Our security defences will be multi-layered and focused on the most important and sensitive assets.

Principle 2: Data-centric security

As a school, our information, particularly pupil data, is a vital asset. Our cyber-security measures will be designed to protect this, first and foremost.

Principle 3: Risk-based approach

Proportionate security measures will be designed based a structured assessment of the threats, risks and vulnerabilities to which key information assets are exposed. Security solutions will be tailored to best protect against these.

Principle 4: Business focused

Information risk management and cyber-security measures will be designed to work in harmony with the needs of the school. Security solutions will be designed using the principle of good commercial practice to ensure efficacy and value for money. The school will ensure that cyber-security is at the heart of all business-driven IT projects.

Principle 5: Emergency preparedness

The school will develop emergency response processes and business continuity plans that will ensure an effective, focused and proportionate reaction to information security and cyber incidents.

Principle 6: Shared responsibility

The school will develop structured mechanisms to raise awareness amongst staff and other stakeholders that responsibility for the security of the school's data rests with everyone. We will demonstrate clear ownership and responsibility for data security within the school.

Strategic Objectives

Objective 1: Information Risk Management

The school should apply the same degree of rigour to assessing the risks to its information assets as it would to legal, regulatory, financial or operational risk. This can be achieved by embedding an information risk management regime across the school, which is actively supported by Governors and the Senior Management Team. Defining and communicating the school's attitude and approach to risk management is crucial.

To achieve this school will:

- Establish a governance framework to enable and support risk management across the organisation, promoting a risk management culture.

- Decide on the level of risk the organisation is prepared to tolerate and communicate it.
- Maintain the Board of Governors' engagement with cyber risk.
- Make cyber risk a regular agenda item within with the oversight of the SMT.
- Record cyber risks in the *Cyber Risk Register* to ensure oversight and ownership.
- Produce supporting risk management policies (the Information Security policy, including an information risk management policy) and review these on a regular basis
- Adopt a life-cycle approach to risk; risk management is a whole life process and the school's policies and processes should support and enable this.
- Ensure that IT suppliers are held accountable via contracts for protecting the personal confidential data they process and meeting the National Data Guardian's Data Security Standard.
- Consider the application of recognised standards of security management good practice (e.g. ISO27000) and implement physical, personnel, procedural and technical measures.
- Educate and maintain users' awareness of risk management within the school.

Objective 2: Network Security

Connecting to untrusted networks (e.g. the internet) exposes the school's networks to attacks that seek to compromise the confidentiality, integrity and availability of Information Technologies (ITs) and the information they store and process. This can be prevented by developing policies and risk management approaches to protect the school's networks by applying security controls that are commensurate with the risks that have been identified and the school's risk appetite.

To achieve this the school will:

- Police the network perimeter and establish multi-layered boundary defences with industry-standard firewalls and web security filters deployed between the untrusted external network and the trusted internal network.
- Limit access to network ports, protocols and applications, filtering and inspecting all traffic at the network perimeter to ensure that only traffic which is required to support the business is being exchanged; control and manage all inbound and outbound network connections and deploy technical controls to scan for malware and other malicious content.
- Deploy firewalls to form a buffer zone between the untrusted external network and the internal network used by the school. The firewall rule set should deny traffic by default and a whitelist should be applied that only allows authorised protocols, ports and applications to communicate with authorised networks and network addresses.
- Prevent malicious content from accessing the network by deploying antivirus and malware-checking solutions to examine both inbound and outbound data at the perimeter, in addition to antivirus and malware protection deployed on internal networks and on host systems. The antivirus and malware solutions used at the perimeter should be different to those used to protect internal networks and systems in order to provide some additional defence in depth.
- Protect the internal network to prevent any direct connections to external services and protect internal IP addresses.

- Identify, group and isolate the school's critical information assets and services and apply appropriate network security controls to them.
- Secure wireless devices: wireless devices should only be allowed to connect to trusted wireless networks, and all wireless access points should be secured. Security scanning tools should have the ability to detect and locate unauthorised wireless access points.
- Implement capabilities to prevent internal IP addresses from being exposed to external networks and attackers and ensure that it is not possible to route network traffic directly from untrusted networks to internal networks.
- Enable secure network administration, ensuring that administrator access to any network component is only carried out over dedicated network infrastructure and secure channels using communication channels that support encryption.
- Ensure that error messages returned to internal or external systems or users do not include sensitive information that may be useful to attackers.
- Monitor network activity: use intrusion monitoring tools and regularly audit activity logs.
- Test the security controls applied to the network: conduct penetration tests, yearly or after any significant change, and undertake simulated cyber-attack exercises.

Objective 3: User Education and Awareness

The use made by staff of the school's Information Technologies (ITs) brings with it various risks. It is critical for all staff to be aware of their personal security responsibilities and the requirement to comply with the school's Information Security Policy. This can be achieved through systematic delivery of a security training and awareness programme that actively seeks to increase the levels of security expertise and knowledge across the school as well as a security-conscious culture.

To achieve this the school will:

- Establish and implement policies covering the acceptable and secure use of the school's systems.
- Establish a staff induction process that includes new users receiving training on their personal security responsibilities.
- Maintain user awareness of the threats posed: all users should receive regular refresher training on the cyber risks to the school.
- Ensure that staff understand their obligations, according to relevant school policies, to handle information responsibly and their personal accountability for deliberate or avoidable breaches.
- Monitor the effectiveness of security training.
- Promote an incident-reporting culture that empowers staff to voice concerns about poor security practices and security incidents without fear or discrimination.
- Ensure that staff are made aware that any abuse of the school's Information Security Policy may result in disciplinary action being taken in line with the school's disciplinary policies.

Objective 4: Malware Prevention

Any information exchange carries a degree of risk as it could expose the school to malicious code and content (malware) which could seriously damage the confidentiality, integrity and availability

of the school's information and Information Technologies (ITs) on which it is hosted. The risk may be reduced by implementing security controls to manage the risks to all business activities.

To achieve this the school will:

- Establish and implement policies to manage the risks posed to the school's processes by malware.
- Ensure that staff understand the risks from malware and the day-to-day procedures that they need to follow to prevent a malware infection from occurring.
- Scan for malware across the organisation: protect all host and client machines with antivirus solutions that will automatically scan for malware.
- Manage all data import and export: all information supplied to or from the school electronically should be scanned for malicious content.
- Black-list malicious websites to block access to known malicious websites.
- Establish anti-malware defences across the school to include:
    - deploying antivirus and malicious code checking solutions with capabilities to continuously scan inbound and outbound objects at the perimeter, on internal networks and on host systems.
    - deploying a content-filtering capability on all external gateways to try to prevent attackers delivering malicious code to the common desktop applications used by the user.
    - Install firewalls on the host and gateway devices and configure them to deny traffic by default, allowing only connectivity associated with known white-listed applications.
    - where school processes can support it, disabling scripting languages such as Windows Scripting, Active X, VBScript and JavaScript.
    - where possible, disabling the 'auto run' function to prevent the automatic import of malicious code from any type of removable media.
    - regularly scanning every network component and applying security patches in compliance with the school's Information Security policy.
    - applying the secure baseline build to every network device and mobile platform.

Objective 5: Removable Media Controls

Failure to control or manage the use of removable media can lead to material financial loss, the theft of information, the introduction of malware and the erosion of the school's reputation.

To achieve this the school will:

- Establish and implement policy to control the use of removable media for the import and export of information.
- Limit the use of removable media to essential areas only, with an approval process in place.
- Scan all removable media for malware: all clients and hosts should automatically scan removable media.
- Scan any media brought into the school for malware with a stand-alone scanner before any data transfer takes place.

- Ensure that all removable media is formally issued by the school to individuals who will be accountable for its secure use.
- Ensure that information held on removable media is encrypted.
- Lock down access to media drives by default and only allow access to approved authorised devices.
- Monitor systems for unauthorised use of removable media.
- Ensure that staff are aware of the risks posed to the school from the use of removable media and their associated personal security responsibilities.

Objective 6: Secure Configuration

By putting in place policies and processes to develop secure baseline builds and manage the configuration and the on-going functionality of all Information Technologies (ITs), the school can greatly improve the security of our systems. It is best practice is to develop a strategy to remove or disable unnecessary functionality from IT systems and keep them patched against known vulnerabilities. Failure to do so is likely to result in increased exposure of the school and its IT to threats and vulnerabilities and therefore increased risk to the confidentiality, integrity and availability of systems and information.

To achieve this the school will:

- Establish and implement polices to update and patch systems, establishing and maintaining policies that set out the priority and timescales for applying updates and patches.
- Create and maintain hardware and software inventories: use automated tools to create and maintain inventories of every device and application used by the school.
- Ensure that no unsupported operating systems, software or internet browsers are used within the IT systems.
- Ensure that where the school remains dependent upon unsupported systems and software to fulfil educational and business objectives additional controls and mitigations are implemented to improve the school's security until the system or software can be removed or de-commissioned.
- Lockdown operating systems and software in line with the business requirements of the school, balancing usability and security.
- Create and implement a baseline security build for workstations, servers, firewalls and routers.
- Conduct regular vulnerability scans: run automated vulnerability scanning tools against all networked devices at least weekly and remedy any vulnerability within an agreed time-frame.
- Produce policies and procedures that define and support the configuration control and change management requirements for all IT systems.
- Disable unnecessary input/output devices and removable media access as dictated by business requirements.

- Limit users' ability to change configurations, providing users with the minimum system rights and permissions they need to fulfil their duties; users with 'normal' privileges should be prevented from installing software.

Objective 7: Manage User Privileges

It is good practice for the school to manage the access privileges that users have to Information Technologies (ITs), the information they hold and the services they provide. All users of IT systems should only be provided with the privileges that they need to do their job. This principle is often referred to as 'Least Privilege'. A failure to manage user privileges appropriately may result in an increase in the number of deliberate and accidental attacks.

To achieve this the school will:

- Establish effective account management processes: manage and review user accounts from creation and modification to eventual deletion.
- Establish pre-employment screening to a level that is commensurate with the sensitivity of the information staff will have access to.
- Ensure that personal confidential data is only accessible to staff who need it for their current role and access is removed as soon as it is no longer required.
- Ensure that all access to personal confidential data on IT systems is attributable to individuals.
- Limit the number and use of privileged accounts.
- Minimise privileges for all users to essential appropriate access: access controls should be allocated on the basis of need and 'Least Privilege'.
- Provide administrators with normal accounts for general use.
- Review the requirement for a privileged account more frequently than standard accounts.
- Monitor user activity, particularly access to sensitive information and the use of privileged account actions.
- Limit access to the audit system and the system activity logs
- Educate users and maintain awareness regarding the school's Acceptable Use Policies.

Objective 8: Incident Management

The school will experience an information security incident at some point. Investment in establishing effective incident management policies and processes will help to improve resilience, support business continuity, improve user and parental confidence and reduce any financial impact.

To achieve this the school will:

- Obtain Senior Management Team approval and backing for incident management; the SMT should lead on the delivery of the incident management plans.
- Establish an incident response and disaster recovery capability.
- Develop and maintain incident management policy and plans with clear roles and responsibilities.

- Ensure that cyber-attacks against services are identified and resisted and security advice is responded to: action is taken immediately following a data breach or a near miss, with a report made to SMT and / or Date Coordinator within 12 hours of detection.
- Ensure that continuity plans are in place to respond to threats to data security, including significant data breaches or near misses, and it is tested once a year as a minimum, with a report to the SMT.
- Establish a systematic approach to the backup of corporate information assets to allow for a data recovery capability, ensuring that backup media is held in secure locations; the ability to recover archived data for operational use should be regularly tested.
- Ensure that processes are reviewed at least annually to identify and improve processes which have caused breaches or near misses, or which force staff to use workarounds which compromise data security.
- Regularly test incident management plans.
- Ensure that all users are aware of their responsibilities and the procedures they should follow to report and respond to an incident.

Objective 9: Remote Working

Remote working offers great business benefit but exposes the school to risks that will be challenging to manage. Mobile working extends the school's security boundary to the user's location. It is advisable for organisations to establish risk-based policies and procedures that cover all types of mobile devices and flexible working if they are to effectively manage the risks. Organisations should also plan for an increase in the number of security incidents and have a strategy in place to manage the loss or compromise of personal and commercially sensitive information and any legal, regulatory or reputational impact that may result.

To achieve this the school will:

- Assess the risks then create and implement a mobile working policy: the policy will cover aspects such as information types, user credentials, devices, encryption and incident reporting.
- Educate users and maintain their awareness about the risks, training them to use their mobile device securely by following appropriate security procedures.
- Ensure that all mobile devices are configured to an agreed secure baseline build.
- Ensure that data is protected at rest: reduce the amount of information stored on a mobile device to the minimum needed when working outside the normal environment and encrypt the data at rest if the device supports it.
- Ensure that data is protected in transit: if the user is working remotely the device and information exchange should be protected by an appropriately configured Virtual Private Network (VPN) or other secure means.

Objective 10: Monitoring

Monitoring Information Technologies (ITs) activity allows the school to better detect attacks and react to them appropriately whilst providing a basis upon which lessons can be learned to improve the overall security of the school. In addition, monitoring the use of IT systems allows the school to

ensure that systems are being used appropriately in accordance with school policies. Monitoring is often a key capability needed to comply with security, legal and regulatory requirements.

To achieve this the school will:

- Establish and implement an organisational monitoring strategy and policy based on an assessment of the risks.
- Monitor all IT systems: ensure that monitoring solutions monitor all networks and host systems (e.g. clients and servers).
- Continuously monitor network traffic to identify unusual activity or trends that could indicate an attack.
- Monitor all user activity: identify unauthorised use or misuse of technology or data; identifying the user, the activity and the information they were attempting to access.
- Ensure that monitoring processes comply with legal or regulatory constraints on the monitoring of user activity
- Provide a resilient and synchronised timing source across the school to time-stamp audit logs, alerts and events.
- Ensure that policies and processes are in place to appropriately manage and respond to incidents detected by monitoring solutions.

Appendix 2: Glossary of cyber security terminology

These key terms will help you to understand the common forms of cyber attack and the measures the school will put in place. They're from the National Cyber Security Centre (NCSC) glossary.

TERM	DEFINITION
Antivirus	Software designed to detect, stop and remove malicious software and viruses.
Breach	When your data, systems or networks are accessed or changed in a non-authorised way.
Cloud	Where you can store and access your resources (including data and software) via the internet, instead of locally on physical devices.
Cyber attack	An attempt to access, damage or disrupt your computer systems, networks or devices maliciously.
Cyber incident	Where the security of your system or service has been breached.
Cyber security	The protection of your devices, services and networks (and the information they contain) from theft or damage.
Download attack	Where malicious software or a virus is downloaded unintentionally onto a device without the user's knowledge or consent.
Firewall	Hardware or software that uses a defined rule set to constrain network traffic – this is to prevent unauthorised access to or from a network.
Hacker	Someone with some computer skills who uses them to break into computers, systems and networks.

TERM	DEFINITION
Malware	Malicious software. This includes viruses, trojans or any code or content that can adversely impact individuals or organisations.
Patching	Updating firmware or software to improve security and/or enhance functionality.
Pentest	Short for penetration test. This is an authorised test of a computer network or system to look for security weaknesses.
Pharming	An attack on your computer network that means users are redirected to a wrong or illegitimate website even if they type in the right website address.
Phishing	Untargeted, mass emails sent to many people asking for sensitive information (such as bank details) or encouraging them to visit a fake website.
Ransomware	Malicious software that stops you from using your data or systems until you make a payment.
Social engineering	Manipulating people into giving information or carrying out specific actions that an attacker can use.
Spear-phishing	A more targeted form of phishing where an email is designed to look like it's from a person the recipient knows and/or trusts.
Trojan	A type of malware/virus designed to look like legitimate software that can be used to hack a victim's computer.
Two-factor/multi-factor authentication	Using 2 or more different components to verify a user's identity.

TERM	DEFINITION
Virus	Programmes designed to self-replicate and infect legitimate software programs or systems.
Virtual private network (VPN)	An encrypted network which allows remote users to connect securely.
Whaling	Highly- targeted phishing attacks (where emails are made to look legitimate) aimed at senior people in an organisation.

Appendix 3: Roles and responsibilities for eSafety

The governing board:

The governing board has overall responsibility for monitoring this policy and holding the headmistress to account for its implementation.

- The governing board will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.
- The governing board will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.
- The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL). • The governing board should ensure children are taught how to keep themselves and others safe, including keeping safe online.
- The governing board must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The board will review the DfE filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting those standards, which include:
    - Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
    - Reviewing filtering and monitoring provisions at least annually;
    - Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;
    - Having effective monitoring strategies in place that meet their safeguarding needs • Governors should ensure that online safety is a running and interrelated theme while devising and implementing their whole school approach to safeguarding and related policies.
- Ensure that they have read and understand this policy.
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet.
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in

all situations, and a more personalised or contextualised approach may often be more suitable

The Head

The Head is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

The safety of all members of the school community, ensuring that sufficient training is in place and accurate reporting procedures.

The designated safeguarding lead (DSL)

Details of the school's DSL and DDSL's are set out in our child protection and safeguarding policy as well as relevant job descriptions. The DSL has responsibility to refer more serious breaches where the wellbeing and safety of a child is seriously compromised to the Police, CEOPS, the Local Prevent Coordinator and local Channel panel as appropriate.

- The DSL takes lead responsibility for online safety in school, in particular:
- Supporting the Head in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the Head, Director of Digital Strategy and Heads of PSHEE and ICT to address any online safety issues or incidents.
- Managing all online safety issues and incidents in line with the school child protection and behaviour policies, making use of MyConcern and the Incidents log.
- Updating and delivering staff training on online safety in conjunction with the Director of Digital Strategy, working with external agencies and external services when necessary.
- Providing reports on online safety as part of their safeguarding remit to the headteacher and governing board after being supplied with relevant information by the Director of Digital Strategy.

The Director of Digital Strategy

- Training the Pastoral Administrator on logging online safety incidents through Lightspeed software and reporting it to DSL to be dealt with appropriately
- Working with the SLT on the promotion of Digital Safeguarding within the PSHEE curriculum, ensuring that key topics of online safety are covered that are relevant to the different year groups and to ensure that this is reviewed annually.
- Provide resources to parents, pupils and staff through online platforms for advice and training.
- Maintain good working knowledge of how generative AI technologies and their misuse could lead to safeguarding threats.

- Maintaining the membership of external organisations to support the online safety provision, keeping updated on the latest findings.

Digital Strategy Group and Technical Staff

Digital Strategy Group and technical staff lead by the Director of Digital Strategy are responsible for:

- Development of best practices and integrating digital governance with other types of governance
- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Responding to updates from relevant bodies (City of London Police, Microsoft etc.) and enacting software patches as necessary
- Conducting a full security check and monitoring the school's ICT systems on a regular basis.
- Running training for staff and pupils on eSafety and cyber security.
- Running regular phishing attack simulations for staff.
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files or non-age appropriate applications.

ICT Department (Academic)

The ICT teachers are responsible for:

- Providing a Computer Science curriculum at KS3 which covers content on the safe and responsible use of the internet and digital technologies.

All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy.
- Implementing this policy consistently.
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet and ensuring that pupils follow the school's terms on acceptable use.
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy and in conjunction with the Behaviour Policy.

- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school Behaviour Policy and logged on MyConcern.
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'.

Parents

Parents are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy.
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet and endorsed this agreement by signature.
- Read all information that is sent by the school with regards to online safety and be responsible for their children's use of technology at home.

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- **UK Safer Internet Centre**
- **Childnet International**
- **Internet Matters**
- **Parent Zone**
- **ThinkUKnow**
- **Parent Info**

Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use.

Appendix 4: eSafety on the curriculum

Computer Science Curriculum

Pupils will be taught about online safety as part of the curriculum. They will be taught how to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

In the first form, pupils use the ThinkUKnow website (run by CEOPS) and also a video that CEOPS created on safety online to learn about the concepts of privacy settings and not over-sharing online.

The second form course is focused on data misuse. Safety online, including protection from phishing, online fraud and malware.

Further discussion about issues surrounding cyber-bullying. Data misuse and Data Protection including Deep Fake technology and bias in algorithms.

Second form AI course deals with plagiarism/misuse of AI and the issues of authenticity arising from the use of generative AI.

PSHEE Curriculum

First Form – Social Media: Positives and Negatives, Phones and Social Media Addiction, Dangers of Posting online (including nudes and semi-nudes), Online Trolls, Scams and Phishing, Dealing with Cyber Bullying, Issues around consumption of pornography, Body image – dangers of media portrayal.

Second Form – Tackling gender stereotypes and media portrayal of gender.

Third Form – Phone Addiction, Effects of tech on health, Cyber bullying, Managing requests to share explicit content, Identifying positive and negative friendship behaviours online, Thinking critically about content posted online (including our responsibility to monitor what we are posting), Online fraud and money mule schemes, Sextortion.

Fourth Form – Impact of Pornography, Issues around sharing or requesting/obtaining sexual images.

Sixth Form – Law around sharing sexual images/Sextortion, Healthy and Unhealthy relationships online, Ways to limit social media use, Online safety and (lack of) anonymity, Avoiding Identity Theft, Maintaining a Positive Online Presence.

Cyber Security workshops

- Pupils will be taught about wider cyber security principles through a series of workshops that are age-appropriate
- Pupils will be given IT privileges on a strict need-to-access basis