Cyber Security & Data Security Policy

Date of issue: May 2018

Review date: May 2021

CONTENTS

Introduction

At Hornchurch High School we see ICT 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, departments build into their Programmes of Study the use of these technologies to arm our young people with the skills to access life-long learning and employment.

Information and Communications Technology covers a wide range of resources including; web-based and mobile learning. We recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Learning Platforms and Virtual Learning Environments
- E-mail and Instant Messaging
- Chat Rooms and Social Networking
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices with web functionality

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies.

At Hornchurch High School, we understand the responsibility to educate our Students on Cyber Security 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.

Our school holds personal data on learners, staff and other people to help us conduct our day-to-day activities. Some of this information is sensitive and could be used by another person or criminal organisation to cause harm or distress to an individual. The loss of sensitive information can result in media coverage, and potentially damage the reputation of our school. This can make it more difficult for our school to use technology to benefit learners.

Everybody in the school has a shared responsibility to secure any sensitive information

used in their day to day professional duties and even staff not directly involved in data handling should be made aware of the risks and threats and how to minimise them.

Both this policy and the Acceptable Use Agreement (for all staff, governors, visitors and students) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, tablets, webcams, whiteboards, voting systems, digital video equipment, etc); and technologies owned by students and staff, but brought onto school premises (such as laptops, mobile phones, camera phones, and portable media players, etc).

Definitions

Cyber Security, within this document the term cyber security will be used to describe both the individual's responsibility for safe use of ICT technologies as well as the school's responsibility to provide a safe and secure system for its staff and students to use.

Data Security, within this document the term data security will be used to describe any personal data that the school use on a day to day basis. Please refer to Hornchurch High School's full GDPR toolkit (an extensive collection of our GDPR policies) for comprehensive information and guidance relating to data protection.

Our Obligation

We the School will provide staff and students with a safe reliable platform that will enable safe use of network and internet services. Since Partnership Learning have been supporting our school we have not sustained any significant cyber-attacks or virus outbreaks.

The way in which we keep our staff and students safe are as follows:

- All our school's internet connections are either via RM internet or LGFL. Both companies mitigate the risk of cyber attacks by multiple layers of security through next generation firewalls. The firewalls provide a host of high-performance threat protection features, including DDoS (distributed denial of service), spam, phishing attacks, data mining, malware and intrusion protection.

- All Partnership Learning schools as a minimum have user based filtering provided by the educational ISPs listed above. This filtering allows granular level filtering of users.

- At our larger schools, in addition to the measures above we also deploy additional on-site security using either Smoothwall or Sophos UTM. These on site solutions offer additional security and increased levels of monitoring.

- We use Microsoft office 365 as our email solution across all of our schools, as part of this solution we have deployed Microsoft's increased security policies to ensure spam and other unwanted emails are stopped at source. We also utilize 2 step authentication to ensure that administrator and other key accounts remain secure.

- Our school networks are mainly CC4 networks from RM and are built with teaching and learning and security in mind.

- All files on our network are secured with NTFS file permissions to ensure access is only granted to the appropriate users.

- All of our schools are covered by onsite Sophos antivirus and firewall. This antivirus is installed on every end-user device.

- All of our on-site servers are regularly patched with the latest RM and Microsoft patches to ensure constant security

Monitoring

Authorised staff may inspect any ICT equipment owned or leased by the School at any time without prior notice. If you are in doubt as to whether the individual requesting such access is authorised to do so, please contact your lead onsite ICT support staff.

Authorised staff may monitor, intercept, access, inspect, record and disclose e-mails, instant messaging, internet/intranet use and any other electronic communications (data or image) involving its employees or contractors, without consent, to the extent permitted by law. This may be to confirm or obtain School business related information; to confirm or investigate compliance with School policies, standards and procedures; to ensure the effective operation of School ICT; for quality control or training purposes; to comply with a Subject Access Request under the Data Protection Act, or to prevent or detect crime.

Authorised staff may, without prior notice, access the e-mail account where applicable, of someone who is absent in order to deal with any business-related issues retained on that account.

All monitoring, surveillance or investigative activities are conducted by authorised staff and comply with the Data Protection Act, the Human Rights Act, the Regulation of Investigatory Powers Act (RIPA) and the Lawful Business Practice Regulations.

Please note that personal communications using School ICT may be unavoidably included in any business communications that are monitored, intercepted and/or recorded.

Breaches

A breach or suspected breach of policy by a School employee, contractor or Student

may result in the temporary or permanent withdrawal of School ICT hardware, software or services from the offending individual.

Any policy breach is grounds for disciplinary action in accordance with the School Disciplinary Procedure or, where appropriate.

Policy breaches may also lead to criminal or civil proceedings.

Incident Reporting

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the lead ICT support representative. Additionally, all security breaches, lost/stolen equipment or data virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must all be reported.

Acceptable Use Agreement: Students

The school has provided computers for use by students. They offer access to a vast amount of information for use in studies, acting like an enormous extension to the school library and offering great potential to support the curriculum.

The computers are provided and maintained for the benefit of all students, who are encouraged to use and enjoy these resources, and ensure they remain available to all. Students are responsible for good behaviour on the Internet just as they are in a classroom or a school corridor. Remember that access is a privilege, not a right and inappropriate use will result in that privilege being withdrawn.

Equipment

- Do not install, attempt to install or store programs of any type on the computers without permission.
- Do not damage, disable, or otherwise harm the operation of computers, or intentionally waste resources.
- Do not use the computers for commercial purposes, e.g. buying or selling goods.
- Do not open files brought in on removable media (such as floppy disks, CDs, flash drives etc.) until they have been checked with antivirus software, and been found to be clean of viruses.
- Do not connect mobile equipment to the network (e.g. laptops, tablet PCs, PDAs etc.) until they have been checked with antivirus software, and been found to be clean of viruses.
- Do not eat or drink near computer equipment.
- The use of USB storage is only permitted if the device is encrypted.

Security and Privacy

- Do not disclose your password to others, or use passwords intended for the use of others.

- Never tell anyone you meet on the Internet your home address, your telephone number, your school's name, or send them your picture, unless you are given permission to do so.
- Do not use the computers in a way that harasses harms, offends or insults others.
- Respect, and do not attempt to bypass, security in place on the computers, or attempt to alter the settings.
- Computer storage areas and floppy disks will be treated like school lockers. Staff may review files and communications to ensure that users are using the system responsibly.

Internet

- Do not access the Internet unless for study or for school authorized / supervised activities.
- Do not use the Internet to obtain, download, send, print, display or otherwise transmit or gain access to materials which are unlawful, obscene or abusive.
- Respect the work and ownership rights of people outside the school, as well as other students or staff. This includes abiding by copyright laws.
- Do not engage in 'chat' activities over the Internet. This takes up valuable resources which could be used by others to benefit their studies.
- Never arrange to meet anyone unless your parent/guardian or teacher goes with you. People you contact online are not always who they seem.

Email

- Be polite and appreciate that other users might have different views from your own. The use of strong language, swearing or aggressive behaviour is not allowed,
- Never open attachments to emails unless they come from someone you already know and trust. They could contain viruses or other programs which would destroy all the information and software on your computer.
- The sending or receiving of email containing material likely to be unsuitable for children or schools is strictly forbidden. This applies to any material of a violent, dangerous, racist, or inappropriate content. Always report such messages to a member of staff.

Please read this document carefully. Only once it has been signed and returned will access to the Internet be permitted. If any student violates these provisions, access to the Internet will be denied and the student will be subject to disciplinary action.

Additional action may be taken by the school in line with existing policy regarding school behaviour. For serious violations, suspension or expulsion may be imposed. Where appropriate, police may be involved or other legal action taken.

Internet Code of Practice Form FOR STUDENTS

- I will only use the internet for appropriate school work.
- I will never tell anyone I meet on the internet my home address, my telephone number or my school's name, unless my teacher specifically gives me permission.
- I will never send anyone my picture without permission from my teacher/parents/carer.
- I will never give my password to anyone else, even my best friend and I will log off when I have finished using the computer.
- I will never arrange to meet anyone in person without first agreeing it with my parents/teacher/carer and get them to come along to the first meeting.
- I will never hang around in an Internet chat room if someone says or writes something which makes me feel uncomfortable or worried, and I will always report it to a teacher or parent.
- I will never respond to unpleasant, suggestive or bullying e-mails or bulletin boards and I will always report it to a teacher or parent.
- I will not look for bad language or distasteful images while I'm online and I will report bad language or distasteful images to a teacher or parent if I come across them accidentally.
- I will always be myself and will not pretend to be anyone or anything I am not.
- I know that my teacher and the Internet service provider will check the sites I have visited!
- I understand that I can access only sites and material relevant to my work in school and that I will not be able to use the Internet if I deliberately look at unsuitable material.
- I understand that I will not be able to use the Internet if I deliberately hack into the schools' network or other systems.
- I know that the posting of anonymous messages and the forwarding of chain messages is not allowed.
- I know that the contents of my e-mail messages will be monitored by the Network Manager
- I may not download software from the Internet (including screen savers, games, video clips, audio clips, *.exe files).

- I know that information on the Internet may not always be reliable and sources may need checking. Web sites may be sponsored by advertisers.

- I will not use e-mail to send or encourage material which is pornographic, illegal, offensive or annoying or invades another person's privacy

Student's Name..... Form Group ……

I have read the Students' Code of Practice and I have discussed it with my son/daughter. We agree to support the school's policy on the use of the Internet.

Signed (Parent/Guardian/Carer) …… ….Student ……..……Date ……..

Acceptable Use Agreement: Staff

The school has provided computers for use by staff. They offer access to a vast amount of information for use in studies, acting like an enormous extension to the school library and offering great potential to support the curriculum.

The computers are provided and maintained for the benefit of all staff, who are encouraged to use and enjoy these resources, and ensure they remain available to all. Remember that access is a privilege, not a right and inappropriate use will result in that privilege being withdrawn.

Equipment

- Do not install, attempt to install, or store programs of any type on the computers without permission.
- Do not damage, disable, or otherwise harm the operation of computers, or intentionally waste resources.
- Do not use the computers for commercial purposes, e.g. buying or selling goods.
- Do not open files brought in on removable media (such as floppy disks, CDs, flash drives etc.) until they have been checked with antivirus software, and been found to be clean of viruses.
- Do not connect mobile equipment to the network (e.g. laptops, tablet PCs, PDAs etc.) until they have been checked with antivirus software, and been found to be clean of viruses.
- Do not eat or drink near computer equipment.
- The use of USB storage is only permitted if the device is encrypted.

Security & Privacy

- Do not disclose your password to others, or use passwords intended for the use of others.
- Never tell anyone you meet on the Internet your home address, your telephone number or your school's name, or send them your picture.
- Do not use the computers in a way that harasses harms, offends or insults others.

- Respect, and do not attempt to bypass, security in place on the computers, or attempt to alter the settings.
- Computer storage areas and floppy disks will be treated like school lockers. Staff may review files and communications to ensure that users are using the system responsibly.

Internet

- Do not access the Internet unless for school activities.
- Do not use the Internet to obtain, download, send, print, display or otherwise transmit or gain access to materials which are unlawful, obscene or abusive.
- Respect the work and ownership rights of people outside the school, as well as other students or staff. This includes abiding by copyright laws.
- Do not engage in 'chat' activities over the Internet. This takes up valuable resources which could be used by others to benefit their studies.

Email

- Be polite and appreciate that other users might have different views from your own. The use of strong language, swearing or aggressive behaviour is not allowed,
- Never open attachments to emails unless they come from someone you already know and trust. They could contain viruses or other programs which would destroy all the information and software on your computer.
- The sending or receiving of email containing material likely to be unsuitable for children or schools is strictly forbidden. This applies to any material of a violent, dangerous, racist, or inappropriate content. Always report such messages to a member of ICT staff.

Please read this document carefully. Only once it has been signed and returned will access to the Internet be permitted.

If any teacher violates these provisions, access to the Internet will be denied and the teacher will be subject to disciplinary action.

Internet Code of Practice Form FOR STAFF

- Staff should always refer to the school's GDPR policies to ensure safe and appropriate use of electronic data
- Staff should be familiar with the school's Network, Internet, e-mail and web site creation policies and the students' code of practice for Internet use.
- Staff should actively monitor what the Students are accessing during lessons.
- Students should have clear guidelines for the content of e-mail messages, sending and receiving procedures.
- Use of the Internet should be supervised by a teacher or adult.
- Students should be taught skills and techniques to enable efficient and effective use of the Internet.
- Students should have a clearly defined focus for using the internet and e-mail.
- If offensive materials are found the monitor should be switched off, any printed materials or portable drives should be confiscated and offensive URLs should be given to the IT Co-ordinator who will report it to the Internet Service Provider.
- Virus protection has been provided by the school as viruses can be downloaded accidentally from the Internet. Students bringing work from home, on usb/portable/pen drives, could also infect the computer - some viruses will cause havoc!
- It is recommended that students do not use social media during lesson times unless directly linked to education.
- Disciplinary action may be taken if the Internet is used inappropriately e.g. for accessing pornographic, racist or offensive material for personal financial gain, gambling, political purposes or advertising.
- Software should not be downloaded from the Internet (including screen savers, games, video clips, audio clips, *.exe files).

I have read the Code of Practice for students and staff and I am familiar with the school's policy on the use of the Internet, e-mail, the creation of web sites and network security.

I agree to abide by these policies and the Teacher's Code of Practice.

Name……Signed……..……Date……..…

Data Security

The accessing and appropriate use of data is something that the Trust and its school takes very seriously.

The school must follow ICO guidelines and must adopt the strict GDPR policies that are managed centrally by Partnership Learning.

Here is a brief overview of our data security procedures, for full information please refer to our Data Protection Policy:

- The School gives all staff access to its Management Information System, with a unique ID and password
- It is the responsibility of everyone to keep passwords secure
- Staff are aware of their responsibility when accessing school data
- Staff have been issued with the relevant guidance documents and the Policy for ICT Acceptable Use
- Leadership have identified a Data Protection Lead.
- Staff keep all school related data secure. This includes all personal, sensitive, confidential or classified data
- Staff should avoid leaving any portable or mobile ICT equipment or removable storage media in unattended vehicles. Where this is not possible, keep it locked out of sight
- It is the responsibility of individual staff to ensure the security of any personal, sensitive, confidential and classified information contained in documents faxed, copied, scanned or printed.

Data Protection Lead

The Data Protection Lead is a senior member of staff who is familiar with information risks and the school's response. they are a member of the senior leadership team and have the following responsibilities:

Purpose of Data Protection Lead
The purpose of School Data Protection Lead (DPL) is to work closely with the Trusts Data Protection Officer (DPO) to ensure that schools within Partnership Learning are compliant with the requirements of the General Data Protection Regulations and Data Protection Bill. The core responsibility of a Data Protection Lead is to oversee a schools data processing practices, ensuring that they meet all statutory requirements, the provision of advice, guidance, and auditing ensuring compliance with the legislation and any requirements of the Information Commissioner, as the Supervisory Authority.

The DPL will remain in regular communication with the Trusts DPO and will ensure that the Trust always has an up to date copy of each schools Data Protection Impact Assessment and associated data audits. To ensure compliance with GDPR regulations the DPLs practices and audits will be compliance checked annually by the Trusts DPO	
Aspects of role	**Desired outcomes**
Data Protection Lead within Schools should advice and develop general staff awareness of Data Protection.	Provide advice, information and training to general school staff population. This training would include, but is not limited to areas such as: • strong password practices • keeping 'portable' data secure • correct use of email • general data protection advice
Work closely with other Data Protection Leads and the Data Protection Officer to support the development of the trusts GDPR practices and delivery of improvements in processes and procedures.	A working party of DPL's from schools will be assembled and will meet throughout the year, chaired by the Trusts DPO. Good practices, breaches and subject access requests will be discussed so that the DPO and the schools DPLs can continue to develop and improve Data protection practices within our schools.
Maintain a full range of reports and audit documentation covering requirements laid out under the GDPR and Data Protection Bill.	The Trust will provide DPLs with a range of templates for reporting and auditing each schools Data and its usage. It is the DPLs responsibility to ensure that these audits and reports are kept up to date and accurate. This information is to be shared with the trusts DPO and will audited annually to ensure compliance.
Act in accordance with all policies and procedures which apply to the role and understand the reasons for this.	Ensure that all policies and procedures in relation to GDPR within The Trust are adhered to.
Perform the role of Data Protection Lead within Hornchurch High School	Monitor compliance with Data Protection legislation and Trust data protection policies, including spot check and audits. Lead on the creation of an Information Asset Register within your school. Ensure the ongoing maintenance of the Information Asset Register as part of any ongoing procurement and development processes.

	Undertake data protection impact assessments and monitor existing projects. Implement and monitor compliance with the School's retention policy. Inform and advise the staff who process personal data of their obligations. Provide awareness-raising and training for school staff on Data Protection (GDPR) and Freedom of Information responsibilities. Advise Headteacher and Trust DPO of Data Protection issues, significant risks and incidents. Investigate Data Protection incidents Be the schools point of contact to individuals whose data is processed on all issues related to the processing of their data and the exercise of their rights under Data Protection legislation
Assist in reviewing, updating and supporting the enforcement of the Trusts Data protection policy / strategy and accompanying standards.	Participate in meetings with other school DPL and Trust DPO to ensure that school data protection policies are fit for purpose and adhered to in accordance to GDPR
Oversee new data projects within the School and ensure compliance.	Ensures the School complies with the privacy by design principles and conducts privacy impact assessments on new data usage
Carry out privacy / data protection impact assessments and review necessary privacy notices as and when required	Ensures Trust approved policies are in place and provided to users of the relevant services Ensures privacy notices are in place that cover: • What information is being collected • Who is collecting it • How is it collected • Why is it being collected • How will it be used • Who will it be shared with • What will be the effect of this on the individuals concerned

Managing e-mails

The use of e-mail within most schools is an essential means of communication for both staff and students. In the context of school, e-mail should not be considered private. Educationally, e-mail can offer significant benefits including; direct written contact between schools on different projects, be they staff based or student based, within school or international. We recognise that students need to understand how to style an e-mail in relation to their age and good network etiquette; 'netiquette' as they have covered this topic in their ICT lessons.

- Where necessary staff can send an encrypted email by using the word 'ENCRYT' in the subject line. The use of 3rd party encryption software is recommended if there is a need for regular encryption.

- The school gives all staff their own e-mail account to use for all school business as a work based tool This is to minimise the risk of receiving unsolicited or malicious e-mails and avoids the risk of personal profile information being revealed

- It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary e-mail histories can be traced. The school email account should be the account that is used for all school business

- Under no circumstances should staff contact students, parents or conduct any school business using personal e-mail addresses

- All e-mails should be checked carefully before sending, in the same way as a letter written on school headed paper

- Students may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes

- E-mails created or received as part of your school job will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000. You must therefore actively manage your e-mail account as follows:

  - Delete all e-mails of short-term value
  - Organise e-mail into folders and carry out frequent house-keeping on all folders and archives

- The forwarding of chain letters is not permitted in school.

- All student e-mail users are expected to adhere to the generally accepted rules of netiquette particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in e-mail communication, or arrange to meet anyone without specific permission, virus checking attachments

- Students must immediately tell a teacher / trusted adult if they receive an offensive e-mail

- Staff must inform the schools lead ICT support representative if they receive an offensive e-mail
- Students are introduced to e-mail as part of the ICT Scheme of Work
- However, you access your school e-mail (whether directly, through webmail when away from the office or on non-school hardware) all the school e-mail policies apply

Equal Opportunities - Students with Additional Needs

The school endeavours to create a consistent message with parents for all students and this in turn should aid establishment and future development of the schools' Cyber Security rules.

However, staff are aware that some students may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of Cyber Security issues.

Where a student has poor social understanding, careful consideration is given to group interactions when raising awareness of Cyber Security. Internet activities are planned and well managed for these children and young people.

Cyber Security in the Curriculum

ICT and online resources are increasingly used across the curriculum. We believe it is essential for Cyber Security guidance to be given to the students on a regular and meaningful basis. Cyber Security is embedded within our curriculum and we continually look for new opportunities to promote Cyber Security.

- The school provides opportunities within a range of curriculum areas to teach about Cyber Security
- Educating Students on the dangers of technologies that maybe encountered outside school is done informally when opportunities arise and as part of the Cyber Security curriculum
- Students are aware of the relevant legislation when using the internet such as data protection and intellectual property which may limit what they want to do but also serves to protect them
- Students are taught about copyright and respecting other people's information, images, etc through discussion, modeling and activities
- Students are aware of the impact of Cyberbullying and know how to seek help if they are affected by any form of online bullying. Students are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/carer, teacher/trusted staff member, or an

organisation such as Childline.

Cyber Security Skills Development for Staff

- Our staff receive regular information on Cyber Security issues in the form of video clips and news bulletins
- New staff receive information on the school's acceptable use policy as part of their induction
- All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of Cyber Security and know what to do in the event of misuse of technology by any member of the school community
- All staff are encouraged to incorporate Cyber Security activities and awareness within their curriculum areas

Incident Reporting, Cyber Security Incident Log

Some incidents may need to be recorded in other places, such as a bullying or racist incident.

Date & time	Name of pupil or staff member	Male or Female	Room and computer/ device number	Details of incident (including evidence)	Actions and reasons

Inappropriate Material

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the lead on site support representative.
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the lead on site support representative, depending on the seriousness of the offence; investigation by the Headteacher/ Trust, immediate

suspension, possibly leading to dismissal and involvement of police for very serious offences.

- Users are made aware of sanctions relating to the misuse or misconduct.

Internet Access - Managing the Internet

The internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people. All use of internet is audited and it is randomly but regularly monitored. Whenever any inappropriate use is detected it will be followed up.

- Our school maintains students who will have supervised access to Internet resources (where reasonable) through the school's fixed and mobile internet technology
- Staff will preview any recommended sites before use
- Raw image searches are discouraged when working with students
- If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents will be advised to supervise any further research
- All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources
- All users must observe copyright of materials from electronic resources

Managing Other Internet Technologies

Internet technologies, including social networking sites, if used responsibly both outside and within an educational context can provide easy to use, creative, collaborative and free facilities. However, it is important to recognise that there are issues regarding the appropriateness of some content, contact, culture and commercialism. To this end, we encourage our students to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.

- At present, our schools endeavors to deny access to social networking sites to all students and staff within our environment.
- All students are advised to be cautious about the information given by others on sites, for example users not being who they say they are
- Students are taught to avoid placing images of themselves (or details within images that could give background details) on such sites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online
- Students are always reminded to avoid giving out personal details on such sites which may identify them or where they are (full name, address, mobile/ home phone numbers, school details, IM/ email address, specific hobbies/ interests)
- Our students are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals
- Students are encouraged to be wary about publishing specific and detailed private thoughts online
- Our Students are asked to report any incidents of bullying to the school
- Staff may only create blogs, wikis or other platforms in order to communicate with students using the LA Learning Platform or other systems approved by the Headteacher

Parental Involvement

We believe that it is essential for parents/ carers to be fully involved with promoting safe use of ICT both in and outside of school and also to be aware of their responsibilities. We regularly consult and discuss Cyber Security and E-Safety with parents/ carers and seek to promote a wide understanding of the benefits related to ICT and associated risks.

- Parents/Carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to school
- Parents/Carers are required to make a decision as to whether they consent to images of their child being taken/ used in the public domain (e.g., on school website)
- Parents/Carers are expected to sign a Home School agreement.

- The school disseminates information to parents relating to Cyber Security where appropriate in the form of;
    - Website/ Learning Platform postings
    - Newsletter items
    - Assembly PowerPoint Slides

Passwords and Password Security

- Always use your own personal passwords to access computer based services
- Make sure you enter your personal passwords each time you logon. Do not include passwords in any automated logon procedures
- Staff should change temporary passwords at first logon
- Change passwords whenever there is any indication of possible system or password compromise
- Do not record passwords or encryption keys on paper or in an unprotected file
- Only disclose your personal password to authorised ICT support staff when necessary, and never to anyone else. Ensure that all personal passwords that have been disclosed are changed once the requirement is finished
- Passwords must contain a minimum of six characters and be difficult to guess
- User ID and passwords for staff and Students who have left the School are removed from the system

If you think your password may have been compromised or someone else has become aware of your password report this to your lead onsite ICT support representative immediately

Remote Access

- You are responsible for all activity via your remote access facility
- Only use equipment with an appropriate level of security for remote access
- To prevent unauthorised access to School systems, keep all access information such IP addresses, logon IDs and PINs confidential and do not disclose them to anyone
- Select passwords/PINs to ensure that they are not easily guessed.
- Avoid writing down or otherwise recording any network access information. Any such information that is written down must be kept in a secure place and disguised so that no other person will be able to identify what it is

- Protect School information and data at all times, including any printed material produced while using the remote access facility. Take particular care when access is from a non-School environment

Safe Use of Images - Taking of Images and Film

REFER TO GDPR POLICIES FOR FULL DETAILS

Digital images are easy to capture, reproduce and publish and, therefore, misuse. We must remember that it is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness.

- With the written consent of parents (on behalf of Students) and staff, the school permits the appropriate taking of images by staff and students with school equipment

- Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of students, this includes when on field trips. However with the express permission of the Headteacher, images can be taken provided they are transferred immediately and solely to the school's network and deleted from the staff device

- Students are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of the others, this includes when on field trips. However, with the express permission of the Headteacher, images can be taken provided they are transferred immediately and solely to the school's network and deleted from the student's device

Consent of Adults Who Work at the School

REFER TO GDPR POLICIES FOR FULL DETAILS

- Permission to use images of all staff who work at the school is sought on induction and a copy is located in the personnel file

Publishing Student's Images and Work

REFER TO GDPR POLICIES FOR FULL DETAILS

On a child's entry to the school, all parents/carers will be asked to give permission to use their child's work/photos in the following ways:

- on the school web site

- on the school's Learning Platform

- in the school prospectus and other printed publications that the school may produce for promotional purposes

- recorded/ transmitted on a video or webcam
- in display material that may be used in the school's communal areas
- in display material that may be used in external areas, i.e. exhibition promoting the school
- general media appearances, eg local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically)

This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue, e.g. divorce of parents, custody issues, etc.

Parents/Carers may withdraw permission, in writing, at any time.

Students' names will not be published alongside their image and vice versa. E-mail and postal addresses of students will not be published. Students' full names will not be published.

Before posting student work on the Internet, a check needs to be made to ensure that permission has been given for work to be displayed.

Storage of Images

REFER TO GDPR POLICIES FOR FULL DETAILS

- Images/ films of children are stored on the school's network
- Rights of access to this material are restricted to the teaching staff and students within the confines of the school network/ Learning Platform

Webcams and CCTV

REFER TO GDPR POLICIES FOR FULL DETAILS

- The school uses CCTV for security and safety. The only people with access to this are designated staff**.** Notification of CCTV use is displayed at the front of the school.
- We do not use publicly accessible webcams in school
- Webcams in school are only ever used for specific learning purposes, i.e. monitoring hens' eggs and never using images of children or adults

Video Conferencing

- Permission is sought from parents and carers if their children are involved in video conferences
- Permission is sought from parents and carers if their children are involved in video conferences with end-points outside of the school
- All students are supervised by a member of staff when video conferencing
- All students are supervised by a member of staff when video conferencing with end-points beyond the school
- The school keeps a record of video conferences, including date, time and participants.
- Approval from the Headteacher is sought prior to all video conferences within school
- The school conferencing equipment is not set to auto-answer and is only switched on for scheduled and approved conferences
- No part of any video conference is recorded in any medium without the written consent of those taking part

School ICT Equipment

- As a user of ICT, you are responsible for any activity undertaken on the school's ICT equipment provided to you
- It is recommended that schools log ICT equipment issued to staff and record serial numbers as part of the school's inventory
- Do not allow your visitors to plug their ICT hardware into the school network points (unless special provision has been made). They should be directed to the wireless ICT Facilities if available
- Ensure that all ICT equipment that you use is kept physically secure
- Do not attempt unauthorised access or make unauthorised modifications to computer equipment, programs, files or data. This is an offence under the Computer Misuse Act 1990
- It is imperative that you save your data on a frequent basis to the school's network drive. You are responsible for the backup and restoration of any of your data that is not held on the school's network drive
- Personal or sensitive data should not be stored on the local drives of desktop PCs. If it is necessary to do so the local drive must be encrypted
- It is recommended that a time locking screensaver is applied to all machines. Any

PCs etc accessing personal data must have a locking screensaver as must any user profiles

- Privately owned ICT equipment should not be used on a school network
- On termination of employment, resignation or transfer, return all ICT equipment to your Manager. You must also provide details of all your system logons so that they can be disabled
- It is your responsibility to ensure that any information accessed from your own PC or removable media equipment is kept secure, and that no personal, sensitive, confidential or classified information is disclosed to any unauthorised person
- All ICT equipment allocated to staff must be authorised by the appropriate Line Manager. Authorising Managers are responsible for:
    - maintaining control of the allocation and transfer within their Unit
    - recovering and returning equipment when no longer needed

Portable & Mobile ICT Equipment

This section covers such items as laptops, Tablets and removable data storage devices. Please refer to the relevant sections of this document when considering storing or transferring personal or sensitive data

- All activities carried out on School systems and hardware will be monitored in accordance with the general policy
- Staff must ensure that all school data is stored on school's network, and not kept solely on the laptop. Any equipment where personal data is likely to be stored must be encrypted
- Equipment must be kept physically secure in accordance with this policy to be covered for insurance purposes. When travelling by car, best practice is to place the laptop in the boot of your car before starting your journey
- Synchronise all locally stored data, including diary entries, with the central school network server on a frequent basis
- Ensure portable and mobile ICT equipment is made available as necessary for anti-virus updates and software installations, patches or upgrades
- The installation of any applications or software packages must be authorised by the ICT support team, fully licensed and only carried out by your ICT support
- In areas where there are likely to be members of the general public, portable or mobile ICT equipment must not be left unattended and, wherever possible, must be kept out of sight

- Portable equipment must be transported in its protective case if supplied

Mobile Technologies

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Many existing mobile technologies such as portable media players, gaming devices, mobile and Smart phones are familiar to children outside of school too.

They often provide a collaborative, well-known device with possible internet access and thus open up risk and misuse associated with communication and internet use. Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed. Our school chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

Personal Mobile Devices (including phones)

- The school allows staff to bring in personal mobile phones and devices for their own use. Under no circumstances does the school allow a member of staff to contact a student or parent/carer using their personal device
- Students are allowed to bring personal mobile devices/phones to school but must not use them for personal purposes within lesson time. At all times the device must be switched onto silent or will be confiscated.
- This technology may be used, however for educational purposes, as mutually agreed with the Headteacher. The device user, in this instance, must always ask the prior permission of the bill payer
- The school is not responsible for the loss, damage or theft of any personal mobile device
- The sending of inappropriate text messages between any member of the school community is not allowed
- Permission must be sought before any image or sound recordings are made on these devices of any member of the school community
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device

Servers

- All our MIS Servers are all managed directly by Capita and are cloud based SIMS
- Always keep servers in a locked and secure environment
- Limit access rights

- Always password protect and lock the server
- Existing servers should have security software installed appropriate to the machine's specification
- Backups should be encrypted by appropriate software
- Data must be backed up regularly
- Back up discs must be securely stored in a fireproof container
- Back up media stored off-site must be secure
- The use of cloud based backups must have high level encryption

Systems and Access

- You are responsible for all activity on school systems carried out under any access/account rights assigned to you, whether accessed via school ICT equipment or your own PC
- Do not allow any unauthorised person to use school ICT facilities and services that have been provided to you
- Use only your own personal logons, account IDs and passwords and do not allow them to be used by anyone else
- Keep your screen display out of direct view of any third parties when you are accessing personal, sensitive, confidential or classified information
- Ensure you lock your screen before moving away from your computer during your normal working day to protect any personal, sensitive, confidential or otherwise classified data and to prevent unauthorised access
- Ensure that you logoff from the PC completely when you are going to be away from the computer for a longer period of time
- Do not introduce or propagate viruses
- It is imperative that you do not access, load, store, post or send from school ICT any material that is, or may be considered to be, illegal, offensive, libelous, pornographic, obscene, defamatory, intimidating, misleading or disruptive to the school or may bring the school into disrepute. This includes, but is not limited to, jokes, chain letters, files, emails, clips or images that are not part of the school's business activities; sexual comments or images, nudity, racial slurs, gender specific comments, or anything that would offend someone on the basis of their age, sexual orientation, religious or political beliefs, national origin, or disability (in accordance with the Sex Discrimination Act, the Race Relations Act and the Disability Discrimination Act)
- Any information held on School systems, hardware or used in relation to School business may be subject to The Freedom of Information Act

- Where necessary, obtain permission from the owner or owning authority and pay any relevant fees before using, copying or distributing any material that is protected under the Copyright, Designs and Patents Act 1998

Review Procedure

There will be an on-going opportunity for staff to discuss any issue of Cyber Security that concerns them

There will be an on-going opportunity for staff to discuss any issue of data security that concerns them

This policy will be reviewed every (12) months and consideration given to the implications for future whole school development planning

The policy will be amended if new technologies are adopted or Central Government change the orders or guidance in any way