E-Safety and ICT Acceptable Use Policy

Category	Statutory
Reviewed by	Headteacher
Approved by and when	Local Governing Body in February 2024
Frequency of review	Annually
Next Review	February 2025

E-Safety and ICT Acceptable Use Policy

Introduction

ICT in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm 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. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies children are using both inside and outside of the classroom include:

- Websites

- E-mail, Instant Messaging and chat rooms

- Social Media, including Facebook and Twitter

- Mobile/ Smart phones with text, video and/ or web functionality

- Other mobile devices with web functionality

- Gaming, especially online

- Learning Platforms and Virtual Learning Environments, including remote lessons

- Blogs and Wikis

- Podcasting

- Video Broadcasting

- Music Downloading

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 and that some have minimum age requirements, usually 13 years.

At Woodlands Park Primary School*,* we understand the responsibility to educate our pupils on e-Safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Schools hold personal data on learners, staff and other people to help them conduct their 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 the school. This can make it more difficult for your 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 pupils) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, mobile devices, webcams, whiteboards, voting systems, digital video equipment, etc.); and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones, and other mobile devices).

Home Learning Devices

The school issues Chromebooks, laptops and Kindle Fire devices to enable children to engage in home learning during school closure or while isolating due to COVID-19 symptoms. Each parent is given an agreement to sign concerning acceptable and safe use of these devices. The devices have parental controls and DfE controls.

Monitoring

Authorised ICT 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 ask for identification. Any ICT authorised staff member will be happy to comply with this request.

ICT authorised staff may monitor, intercept, access, inspect, record and disclose telephone calls, e-mails, instant messaging, internet/intranet use and any other electronic communications (data, voice 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 1998, or to prevent or detect crime.

ICT authorised staff may, without prior notice, access the e-mail or voice-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 ICT authorised staff and comply with the Data Protection Act 1998, the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000 (RIPA) and the Lawful Business Practice Regulations 2000.

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 pupil 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, the HCC Disciplinary Procedure or Probationary Service Policy.

Policy breaches may also lead to criminal or civil proceedings.

The ICO's new powers to issue monetary penalties came into force on 6 April 2010, allowing the Information Commissioner's office to serve notices requiring organisations to pay up to £500,000 for serious breaches of the Data Protection Act.

The data protection powers of the Information Commissioner's Office are to:

- Conduct assessments to check organisations are complying with the Act;

- Serve information notices requiring organisations to provide the Information Commissioner's Office with specified information within a certain time period;
- Serve enforcement notices and 'stop now' orders where there has been a breach of the Act, requiring organisations to take (or refrain from taking) specified steps in order to ensure they comply with the law;
- Prosecute those who commit criminal offences under the Act;
- Conduct audits to assess whether organisations processing of personal data follows good practice,
- Report to Parliament on data protection issues of concern

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 school's Head Teacher and School Business Manager. Additionally, all security breaches, lost/stolen equipment or data (including remote access SecureID tokens and PINs), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to your Head Teacher.

Online Sessions/Remote Learning:

There may be times when children need to access the classroom learning environment from their own home due to the school only being open to a selection of pupils (Eg during a National Lockdown where schools are closed to the majority of pupils). During this time, children and parents/carers must abide by the Remote Learning Protocol:

- Children, parents and carers should not share invite links or passcodes with anyone to avoid any unauthorised persons joining an online session.
- Parents should always be present during online sessions.
- Cameras will only be used where it is necessary for the children to see the teacher and the teacher to see the children.
- Children should be appropriately dressed and all parents, carers, siblings and other members of the household should be appropriately dressed and be mindful that they could be seen/heard by others.

- Children should be paying full attention to the session and not be eating/watching television/playing on devices/lying in bed.
- If asked by the teacher/member of staff leading the session, they should mute and/or turn off the camera if asked.
- Teachers, should where possible have another member of staff present at the session.
- Members of staff, children, parents and carers should be aware of their responsibility to report anything they see or hear which may pose a safeguarding risk. Members of staff should report any concerns to the Designated Safeguarding Lead (Wendy Philps) or one of the deputies.
- Acceptable Use Agreement:

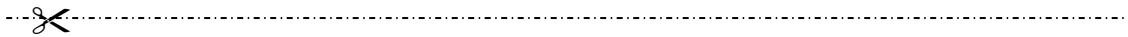**Primary Pupil Acceptable Use
Agreement / eSafety Rules**

- I will only use IT in school for school purposes.

- I will only use my class e-mail address or my own school e-mail address when e-mailing.

- I will only open e-mail attachments from people I know, or who my teacher has approved.

- I will not tell other people my ICT passwords.

- I will not use anyone else's login and/or passwords.

- I will only open/delete my own files.

- I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.

- I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will tell my teacher immediately.

- I will not give out my own details such as my name, phone number or home address. I will not arrange to meet someone unless this is part of a school project approved by my teacher and a responsible adult comes with me.

- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.

- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community.

- I will not use private messaging, groups such as WhatsApp, Messenger etc to send messages, images, video, sounds or text that could upset any member of the school community.

- I know that my use of ICT can be checked and that my parent/ carer contacted if a member of school staff is concerned about my eSafety.

- If I have been given a device for home learning, I will abide by the agreement signed for acceptable and safe use.

Dear Parent/ Carer

ICT including the internet, e-mail and mobile technologies has become an important part of learning in our school.   We expect all children to be safe and responsible when using any ICT.

Please read and discuss these eSafety rules with your child and return the slip at the bottom of this page.

--------✂--

Parent/ carer signature
We have discussed this and …………………………………............(child name) agrees to follow the eSafety rules and to support the safe use of ICT at Woodlands Park Primary and Nursery School.

Parent/ Carer Signature …………………………………………………….

Class ………………………………. Date ……………………………

E-Safety and ICT Acceptable Use Policy

Acceptable Use Agreement: Staff, Governors and Visitors
Staff, Governor and Visitor
Acceptable Use Agreement / Code of Conduct

IT (including data) and the related technologies such as e-mail, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with The Head.

- I will only use the school's email / Internet / Intranet and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body.
- I will always sign into a device with my own username and password
- I will comply with the IT system security and not disclose any passwords provided to me by the school or other related authorities
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number and personal e-mail address, to pupils.
- I will only use the approved, secure e-mail system(s) for any school business.
- I will ensure that personal data (such as data held on MIS software) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body. Personal or sensitive data taken off site must be encrypted.
- I will not install any hardware of software without permission
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and/ or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Head teacher.

- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the school community
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to the Head teacher.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute. This includes making comments or expressing any views on social media which may damage my professional reputation or the reputation of the school.
- I will support and promote the school's e-Safety and Data Security policies and help pupils to be safe and responsible in their use of IT and related technologies. I agree to follow this code of conduct and to support the safe and secure use of IT throughout the school.

Signature ………………………..…………… Date ……………………

Job title ……………………………………..………..

Staff Professional Responsibilities

PROFESSIONAL RESPONSIBILITIES
When using any form of ICT, including the Internet, in school and outside school

For your own protection we advise that you:

> Ensure all electronic communication with pupils, parents, carers, staff and others is compatible with your professional role and in line with school policies.

> Do not talk about your professional role in any capacity when using social media such as Facebook and YouTube.

> Do not put online any text, image, sound or video that could upset or offend any member of the whole school community or be incompatible with your professional role.

> Use school ICT systems and resources for all school business. This includes your school email address, school mobile phone and school video camera.

> Do not give out your own personal details, such as mobile phone number, personal e-mail address or social network details to pupils, parents, carers and others.

> Do not disclose any passwords and ensure that personal data (such as data held on MIS software) is kept secure and used appropriately.

> Only take images of pupils and/ or staff for professional purposes, in accordance with school policy and with the knowledge of SLT.

> Do not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.

> Ensure that your online activity, both in school and outside school, will not bring your organisation or professional role into disrepute.

You have a duty to report any eSafety incident which may impact on you, your professionalism or your organisation.

The HSCB eSafety subgroup group have produced a clear summary of **professional responsibilities related to the use of ICT** which has been endorsed by unions. To download visit http://www.thegrid.org.uk/eservices/safety/policies.shtml
Computer Viruses

- All files downloaded from the Internet, received via e-mail or on removable media such as a memory stick, must be checked for any viruses using school provided anti-virus software before being used

- Never interfere with any anti-virus software installed on school IT equipment that you use

- If your machine is not routinely connected to the school network, you must make provision for regular virus updates through your IT team

- If you suspect there may be a virus on any school IT equipment, stop using the equipment and contact your IT support provider immediately. The IT support provider will advise you what actions to take and be responsible for advising others that need to know

e-Mail

The use of e-mail within most schools is an essential means of communication for both staff and pupils. 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 pupil based, within school or international. We recognise that pupils need to understand how to style an e-mail in relation to their age and good network etiquette; 'netiquette'. In order to achieve IT level 4 or above, pupils must have experienced sending and receiving e-mails.

Managing e-Mail

- The school gives all staff their own e-mail account to use for all school business as a work based tool This is to protect staff, 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 pupils, parents or conduct any school business using personal e-mail addresses

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

- Staff sending e-mails to external organisations, parents or pupils are advised to cc. the Head Teacher

- Pupils 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

- All pupil 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

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

- Staff must inform the Head teacher or ICT Coordinator if they receive an offensive e-mail

- Pupils 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

12

Sending e-Mails

- If sending e-mails containing personal, confidential, classified or financially sensitive data to external third parties or agencies, refer to the Section emailing Personal, Sensitive, Confidential or Classified Information

- Use your own school e-mail account so that you are clearly identified as the originator of a message

- Keep the number and relevance of e-mail recipients, particularly those being copied, to the minimum necessary and appropriate

- Do not send or forward attachments unnecessarily. Whenever possible, send the location path to the shared drive rather than sending attachments

- School e-mail is not to be used for personal advertising

Receiving e-Mails

- Check your e-mail regularly

- Activate your 'out-of-office' notification when away for extended periods

- Never open attachments from an untrusted source; Consult your network manager first

- Do not use the e-mail systems to store attachments. Detach and save business related work to the appropriate shared drive/folder

- ☐ The automatic forwarding and deletion of e-mails is not allowed **e-mailing**

Personal, Sensitive, Confidential or Classified Information

- ☐ Where your conclusion is that e-mail must be used to transmit such data:

  - ☐ Obtain express consent from your manager to provide the information by e-mail

- Exercise caution when sending the e-mail and always follow these checks before releasing the e-mail:

  - Verify the details, including accurate e-mail address, of any intended recipient of the information
  - Verify (by phoning) the details of a requestor before responding to email requests for information
  - Do not copy or forward the e-mail to any more recipients than is absolutely necessary

- Do not send the information to anybody/person whose details you have been unable to separately verify (usually by phone)
- Send the information as an encrypted document **attached** to an e-mail
- Provide the encryption key or password by a **separate** contact with the recipient(s)
- Do not identify such information in the subject line of any e-mail ☐ Request confirmation of safe receipt

.

Equal Opportunities

Pupils with Additional Needs

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

However, staff are aware that some pupils may require additional support or teaching including adapted resources, reminders, prompts and further explanation to reinforce their existing knowledge and understanding of eSafety issues.

Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of eSafety. Internet activities are planned and well managed for these children. **eSafety - Roles and Responsibilities**

As eSafety is an important aspect of strategic leadership within the school, the Head and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named eSafety co-ordinator in this school is Head teacher /ICT Coordinator who has been designated this role as a member of the senior leadership team. All members of the school community have been made aware of who holds this post. It is the role of the eSafety co-ordinator to keep abreast of current issues and guidance through organisations such as Herts LA, CEOP (Child Exploitation and Online Protection) and Childnet.

Senior Management and governors are updated by the Head/ eSafety co-ordinator and all governors have an understanding of the issues and strategies at our school in relation to local and national guidelines and advice.

This policy, supported by the school's acceptable use agreements for staff, governors, visitors and pupils, is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: child protection, health and safety, home–school agreements, and behaviour/pupil discipline (including the anti-bullying) policy and PSHE

eSafety in the Curriculum

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

- The school has a framework for teaching internet skills in ICT/ PSHE lessons

- The school provides opportunities within a range of curriculum areas to teach about eSafety

- Educating pupils about the online risks that they may encounter outside school is done informally when opportunities arise and as part of the eSafety curriculum, including material which promotes radical and extreme views and is contrary to British Values.

- Pupils 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

- Pupils are taught about copyright, respecting other people's information, safe use of images and other important areas through discussion, modeling and appropriate activities

- Pupils are aware of the impact of Cyber bullying and know how to seek help if they are affected by any form of online bullying. Pupils 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 Cybermentors, Childline or CEOP report abuse button

- Pupils are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the ICT curriculum

eSafety Skills Development for Staff

- New staff receive information on the school's acceptable use policy as part of their induction

- All staff have been made aware of their individual responsibilities relating to the safeguarding of children within the context of eSafety and know what to do in the event of misuse of technology by any member of the school

- All staff are encouraged to incorporate eSafety activities and awareness within their curriculum areas

Incident Reporting, eSafety Incident Log & Infringements

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 Head teacher / ICT Coordinator. Additionally, all security breaches, lost/stolen equipment or data (including remote access SecureID tokens and PINs), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported **eSafety Incident Log**

Keeping an incident log can be a good way of monitoring what is happening and identify trends or specific concerns.

'School name' eSafety Incident Log

Details of ALL eSafety incidents to be recorded by the eSafety Coordinator. This incident log will be monitored termly by the Headteacher, Member of SLT or Chair of Governors. Any incidents involving Cyberbullying may also need to be recorded elsewhere

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

This can be downloaded
http://www.thegrid.org.uk/eservices/safety/research/incident.shtml

Misuse and Infringements

Complaints
Complaints and/ or issues relating to eSafety should be made to the Head teacher. .

Inappropriate Material
- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the Head teacher
- Deliberate access to inappropriate materials by any user will lead to the incident being logged and depending on the seriousness of the offence; investigation by the Head teacher/ LA. Infringements could lead to 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

The internet is an open worldwide communication medium, available to everyone 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.

Managing the Internet

- The school provides pupils with supervised access to Internet resources (where reasonable) through the school's fixed and mobile internet connectivity

- Staff will preview any recommended sites before use

- Raw image searches are discouraged when working with pupils

- 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

Internet Use

- You must not post personal, sensitive, confidential or classified information or disseminate such information in any way that may compromise the intended restricted audience

- Do not reveal names of colleagues, pupils, others or any other confidential information acquired through your job on any social networking site or other online application

- On-line gambling or gaming is not allowed

It is at the Head teacher's discretion as to what internet activities are permissible for staff and pupils

Infrastructure

- RBWM has a monitoring solution via the Grid for Learning where web-based activity is monitored and recorded

- School internet access is controlled through the LA's web filtering service.

- Woodlands Park Primary and Nursery School is aware of its responsibility when monitoring staff communication under current legislation and takes into account; Data Protection Act 1998, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000, Human Rights Act 1998

- Staff and pupils are aware that school based email and internet activity can be monitored and explored further if required

- The school does not allow pupils access to internet logs

- If staff or pupils discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the teacher

- It is the responsibility of the school, by delegation to the network manager, to ensure that anti-virus protection is installed and kept up-to-date on all school machines

- Pupils and Staff using personal removable media are responsible for measures to protect against viruses, for example making sure that additional systems used have up-to-date virus protection software. It is not the school's responsibility nor the network managers to install or maintain virus protection on personal systems. If pupils wish to bring in work on removable media it must be given to the teacher for a safety check first

- Pupils and staff are not permitted to download programs or files on school based technologies without seeking prior permission from the Head teacher/ ICT Coordinator

- If there are any issues related to viruses or anti-virus software, the network manager should be informed

Managing Other Web 2 Technologies

Online 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 pupils to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.

- At present, the school endeavors to deny access to social networking and online games websites to pupils within school

- All pupils are advised to be cautious about the information given by others on such websites, for example users not being who they say they are

- Pupils are taught to avoid placing images of themselves (or details within images that could give background details) on such websites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online

- Pupils are always reminded to avoid giving out personal details on websites which may identify them or where they are (full name, address, mobile/ home phone numbers, school details, IM/ email address, specific hobbies/ interests)

- Our pupils are advised to set and maintain their online profiles to maximum privacy and deny access to unknown individuals

- Pupils are encouraged to be wary about publishing specific and detailed private thoughts and information online

- Our pupils are asked to report any incidents of Cyber bullying to the school

- Staff may only create blogs, wikis or other online areas in order to communicate with pupils using the school learning platform or other systems approved by the Head teacher

Parental Involvement

We believe that it is essential for parents/carers to be fully involved with promoting eSafety both in and outside of school and to be aware of their responsibilities.   We regularly consult and discuss eSafety with parents/ carers and seek to promote a wide understanding of the benefits of new technologies together with the associated risks.

- Parents/carers and pupils are actively encouraged to contribute to adjustments or reviews of the school eSafety policy

- Parents/carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to the school

- Parents/carers are required to make a decision as to whether they consent to images of their child being taken and used in the public domain (e.g., on school website)

- Parents/carers are expected to sign a Home School agreement containing the following statement or similar

    - **We will support the school approach to on-line safety and not deliberately upload or add any text, image, sound or video that could upset or offend any member of the school community**

Passwords and Password Security

Passwords

- **Always use your own** personal passwords

- 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

- **Never tell a child or colleague your password**

If you are aware of a breach of security with your password or account inform the Head teacher / IT Coordinator immediately

- Passwords must contain a minimum of six characters and be difficult to guess.

- Passwords should contain a mixture of upper and lowercase letters, numbers and symbols

- User ID and passwords for staff and pupils who have left the school are removed from the system within 1 year

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

Password Security

Password security is essential for staff, particularly as they are able to access and use pupil data. Staff are expected to have secure passwords which are not shared with anyone. The pupils are expected to keep their passwords private and not to share with others, particularly their friends. Staff and pupils are regularly reminded of the need for password security.

- All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's eSafety Policy and Data Security

- Users are provided with an individual network, email log-in username.

- Pupils are not allowed to deliberately access on-line materials or files on the school network, of their peers, teachers or others

- Staff are aware of their individual responsibilities to protect the security and confidentiality of the school networks, MIS systems and/or learning platform, including ensuring that passwords are not shared and are changed periodically. Individual staff users must also make sure that workstations are not left unattended and are locked.

Zombie Accounts

Zombie accounts refers to accounts belonging to users who have left the school and therefore no longer have authorised access to the school's systems. Such Zombie accounts when left active can cause a security threat by allowing unauthorised access.

- Ensure that all user accounts are disabled once the member of the school has left

- Prompt action on disabling accounts will prevent unauthorized access

- Regularly change generic passwords

Safe Use of Images

Taking of Images and Film

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 pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment

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

- Pupils are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of pupils, staff and others without advance permission from the Head teacher

- Pupils and staff must have permission from the Head teacher before any image can be uploaded for publication

Consent of Adults Who Work at the School

- 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 Pupil's Images and Work

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

- 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, ie 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, eg divorce of parents, custody issues, etc.

Parents or carers may withdraw permission, in writing, at any time. Consent has to be given by both parents in order for it to be deemed valid.

Pupils' names will not be published alongside their image and vice versa. E-mail and postal addresses of pupils will not be published. Pupils' 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

- Images/ films of children are stored on the school's network
- Pupils and staff are not permitted to use personal portable media for storage of images (e.g., USB sticks) without the express permission of the Head teacher

- Rights of access to this material are restricted to the teaching staff and pupils within the confines of the school network or other online school resource

- Teachers have the responsibility of deleting the images when they are no longer required, or when the pupil has left the school

School ICT Equipment including Portable & Mobile IT Equipment & Removable Media

School ICT Equipment

- As a user of the school IT equipment , you are responsible for your activity

- It is recommended that schools log IT 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

- Ensure that all IT 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 network. You are responsible for the backup and restoration of any of your data that is not held on the school's network .

- Personal or sensitive data should not be stored on the local drives of desktop PC, laptop, USB memory stick, or other portable device. If it is necessary to do so the local drive must be encrypted

- Privately owned IT equipment should not be used on a school network

- On termination of employment, resignation or transfer, return all equipment. 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:

  o maintaining control of the allocation and transfer within their Unit o recovering and returning equipment when no longer needed

- All redundant ICT equipment is disposed of in accordance with Waste Electrical and Electronic Equipment (WEEE) directive and Data Protection Act (DPA)

Portable & Mobile ICT Equipment

This section covers such items as laptops, mobile devices 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 the school 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. Mobile technologies such as, Smartphones, Blackberries, iPads, games players are generally very familiar to children outside of school. 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 pupil or parent/ carer using their personal device. There are circumstances (such as the DSL during lockdown) where a member of staff needs to contact a family using their own personal telephone. Number withheld should be used.

- Pupils are allowed to bring personal mobile devices/phones but they must be handed in to the office upon arrival and collected at the end of the day.

- This technology may be used for educational purposes, as mutually agreed with the Head teacher. 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

School Provided Mobile Devices (including phones)

- 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 the devices of any member of the school community

- Where the school provides mobile technologies such as phones, laptops and iPads for offsite visits and trips, only these devices should be used

- Where the school provides a laptop for staff, only this device may be used to conduct school business outside of school

Removable Media

If storing or transferring personal, sensitive, confidential or classified information using Removable Media

- Always consider if an alternative solution already exists
- Only use recommended removable media
- Store all removable media securely
- Removable media must be disposed of securely by your ICT support team

Smile and Stay Safe Poster eSafety guidelines to be displayed throughout the school

SMILE and stay safe

Staying safe means keeping your personal details private, such as full name, phone number, home address, photos or school. Never reply to ASL (age, sex, location)

Meeting up with someone you have met online can be dangerous. Only meet up if you have first told your parent or carer and they can be with you

Information online can be untrue, biased or just inaccurate. Someone online my not be telling the truth about who they are - they may not be a 'friend' **L**et a parent, carer, teacher or trusted adult know if you ever feel worried, uncomfortable or frightened about something online or someone you have met or who has contacted you online

Emails, downloads, IM messages, photos and anything from someone you do not know or trust may contain a virus or unpleasant message. So do not open or reply

Social Media, including Facebook and Twitter

Facebook, Twitter and other forms of social media are increasingly becoming an important part of our daily lives.

- Staff are not permitted to access their personal social media accounts using school equipment at any time. The school has a Facebook Page for Parents and school staff may need to access their FB account to post on the Parent FB page.

- Pupils are not permitted to access their social media accounts whilst at school

- Staff, governors, pupils, parents and carers are regularly provided with information on how to use social media responsibly and what to do if they are aware of inappropriate use by others

- Staff, governors, pupils, parents and carers are aware that the information, comments, images and video they post online can be viewed by others, copied and stay online forever

- Staff, governors, pupils, parents and carers are aware that their online behaviour should at all times be compatible with UK law

Telephone Services

Mobile Phones (where appropriate)

- You are responsible for the security of your school mobile phone. Always set the PIN code on your school mobile phone and do not leave it unattended and on display (especially in vehicles)

- Report the loss or theft of any school mobile phone equipment immediately

- The school remains responsible for all call costs until the phone is reported lost or stolen

- You must read and understand the user instructions and safety points relating to the use of your school mobile phone prior to using it

- School SIM cards must only be used in school provided mobile phones

- All school mobile phones are barred from calling premium rate numbers and any numbers outside of the UK as the default

- You must not send text messages to premium rate services

- In accordance with the **Finance policy** on the private use of school provided mobiles, you must reimburse the school for the cost of any personal use of your school mobile phone. This includes call charges incurred for incoming calls whilst abroad. [To assist you in identifying personal use, add * to the end of the number being contacted, these will be shown separately on your bill]. Payment arrangements should be made through your finance administrator

- Never use a hand-held mobile phone whilst driving a vehicle. Only genuine 999 or 112 emergency calls may be made if it would be unsafe to stop before doing so

Current Legislation

Acts Relating to Monitoring of Staff email

Data Protection Act (GDPR) 2018

The Act requires anyone who handles personal information to comply with important data protection principles when treating personal data relating to any living individual. The Act grants individuals right of access to their personal data, compensation and prevention of processing. https://www.gov.uk/data-protection

The Telecommunications (Lawful Business Practice)

(Interception of Communications) Regulations 2000
http://www.hmso.gov.uk/si/si2000/20002699.htm

Regulation of Investigatory Powers Act 2000

Regulating the interception of communications and making it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998. The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, however, permit a degree of monitoring and record keeping, for example, to ensure communications are relevant to school activity or to investigate or detect unauthorised use of the network. Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored. Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation.

http://www.hmso.gov.uk/acts/acts2000/20000023.htm

Human Rights Act 1998 http://www.hmso.gov.uk/acts/acts1998/19980042.htm

Other Acts Relating to eSafety

Racial and Religious Hatred Act 2006

It a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Sexual Offences Act 2003

The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust.   Schools should already have a copy of "*Children & Families: Safer from Sexual Crime*" document as part of their child protection packs. For more information www.teachernet.gov.uk

Communications Act 2003 (section 127)

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

The Computer Misuse Act 1990 (sections 1 – 3)

Regardless of an individual's motivation, the Act makes it a criminal offence to gain:

- access to computer files or software without permission (for example using another person's password to access files)

- unauthorised access, as above, in order to commit a further criminal act (such as fraud)

- impair the operation of a computer or program

UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

Malicious Communications Act 1988 (section 1)

This legislation makes it a criminal offence to send an electronic message (e-mail) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.

Copyright, Design and Patents Act 1988

Copyright is the right to prevent others from copying or using work without permission. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer. Copyright infringement is to copy all or a substantial part of anyone's work without obtaining them author's permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else's material. It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.

Public Order Act 1986 (sections 17 – 29)

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

Protection of Children Act 1978 (Section 1)

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is a anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

Obscene Publications Act 1959 and 1964

Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other.

A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Acts Relating to the Protection of Personal Data

General Data Protection Regulations (GDPR) 2018 https://www.gov.uk/data-protection

The Freedom of Information Act 2000
http://www.ico.gov.uk/for_organisations/freedom_of_information_guide.aspx