Rochford Primary and Nursery School (Academy)

E-safety and Data Security Policy

(to be read in conjunction with all GDPR Policies)
Vision Statement:

“Inspiring lifelong learning”

We are committed to providing:

• inspirational teaching;

• a stimulating environment;

• a challenging and interesting curriculum, so that children learn a variety of skills and are inspired to develop a love of learning; and

• a happy, safe and caring school where:
  
  - every child can reach their full potential
  
  - staff are valued
  
  - visitors feel welcome.

We are committed to developing an inclusive school at the heart of the Rochford Community where:

• every child’s happiness and needs are of great importance;

• where there are high expectations of good behaviour; and

• where all members of the school community value good manners and co-operation.

We are committed to:

• communicating and working effectively with parents so that there is a genuine partnership supporting children’s learning.
Introduction

ICT in the 21st Century is 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 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 Rochford Primary and Nursery School we understand the responsibility to educate our pupils on eSafety 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 the 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,
personal digital assistants (PDAs), tablets, 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, camera phones, PDAs and portable media players, etc).

**Monitoring**

Authorised ICT staff may inspect any ICT equipment owned or leased by the School at any time without prior notice.

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 2018, or to prevent or detect crime.

ICT authorised staff may, without prior notice, access the school 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 2018, 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.

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 Essex County Council Disciplinary Procedure.

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 school’s Computing Lead. Additionally, all security breaches, lost/stolen equipment or data (including remote access Secure ID tokens and PINs), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported either the Computing Lead or the Office Manager.
Rochford Primary and Nursery School

Acceptable Use Agreement:

Pupils e-Safety Rules

• I will only use ICT 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 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 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 e-Safety.
ICT (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 of School.

➢ I will only use the school’s technological resources for professional purposes or for uses deemed ‘reasonable’ by the Headteacher or Local Governing Body.
➢ I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities
➢ I will ensure that all electronic communications are compatible with my professional role.
➢ I will not give out my own personal details, such as mobile phone number, personal e-mail address and social networking identities 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 Headteacher or Local Governing Body. Personal or sensitive data taken off site must be encrypted.
➢ I will not install any hardware or software without permission of the Head of School.
➢ 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 the 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 Headteacher.
➢ 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 my Line Manager or Headteacher.
➢ 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.
➢ To this end I will not use social media in school; when I use social media out of school I will set security measures at high; I will not discuss school matters on social media.
➢ 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 ICT and related technologies.
➢ I understand this forms part of the terms and conditions set out in my contract of employment.

This Acceptable Use Agreement is a summary of our E-Safety Policy which is available in full on our website/on request.

User Signature

I agree to follow this code of conduct and to support the safe and secure use of ICT throughout the school

Signature ............................................. Date .................................

Full Name ................................................................. (printed) Job title ..................................
Computer Viruses

- All files downloaded from the Internet, received via e-mail or on removable media (e.g. USB stick) must be checked for any viruses using school provided anti-virus software before using them.
- Never interfere with any anti-virus software installed on school ICT equipment that you use.
- If your machine is not routinely connected to the school network, you must make provision for regular virus updates through the ICT Lead.
- If you suspect there may be a virus on any school ICT equipment, stop using the equipment and contact the Computing Lead or Headteacher immediately. The Computing Lead or Headteacher will advise you what actions to take and be responsible for advising others that need to know.

Security

- The School gives relevant 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.
- Staff have read the relevant guidance documents available on the EGfL website.
- The Leadership Team has identified the Senior Information Risk Owner (Headteacher) and the Asset Information Owner (Office Manager).
- Staff will 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 e-mailed, faxed, copied, scanned or printed.

Disposal of Redundant ICT Equipment Policy

- All redundant ICT equipment will be disposed of through an authorised agency only and in accordance with the SEEAT Financial Regulations. This should include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.
- All redundant ICT equipment that may have held personal data will have the storage media wiped.
- The school will maintain a comprehensive inventory of all its ICT equipment including a record of disposal.
- Any redundant ICT equipment being considered for sale / gift will have been subject to a recent electrical safety check and hold a valid PAT certificate.
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 ICT 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 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.

- The school requires a standard disclaimer to be attached to all e-mail correspondence, stating that, ‘the views expressed are not necessarily those of the school or of SEEAT. The responsibility for adding this disclaimer lies with the account holder.

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

- 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 housekeeping on all folders and archives

- All children use a class/group e-mail address.

- 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 Computing Lead / line manager) if they receive an offensive e-mail.

- Pupils are introduced to e-mail as part of the Computing 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.
• The use of Hotmail, BT Internet, GMail or any other Internet based webmail service for sending, reading or receiving business related e-mail is not permitted.

**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 E-mailing 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. Or staff may use the Drop Box facility.

• An outgoing e-mail greater than ten megabytes (including any attachments) is likely to be stopped automatically. This size limit also applies to incoming e-mails.

**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**

• As far as possible do not send this sort of information by e-mail.

• 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:
    
    o Verify the details, including accurate e-mail address, of any intended recipient of the information
    o Do not copy or forward the e-mail to any more recipients than is absolutely necessary
  
  – 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) – preferably by telephone
  – Do not identify such information in the subject line of any e-mail
  – Request confirmation of safe receipt
In exceptional circumstances, the County Council makes provision for secure data transfers to specific external agencies. Such arrangements are currently in place with:

- Essex Police
- District and Borough Councils within Essex County Council
- Essex NHS Trusts

**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 school’s e-Safety rules.

However, staff are aware that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of e-Safety issues.

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

**E-Safety - Roles and Responsibilities**

As e-Safety 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 e-Safety Lead in this school is the Computing Lead.

Senior Management and Governors are updated by the Headteacher 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 and harassment) policy and PSHE.

**E-Safety in the Curriculum**

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

- The school has a framework for teaching internet skills in its ICT “Non-negotiables” document.

- Educating pupils on the dangers of technologies that may be encountered outside school is done informally when opportunities arise and as part of the e-Safety curriculum

- Pupils in Years 4, 5 and 6 are aware of the impact of Cyberbullying 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 Child line or CEOP report abuse button.
E-Safety Skills Development for Staff

- Our staff will receive regular information and training on e-Safety issues in the form of staff meetings and courses.
- New staff will receive information on the school’s acceptable use policy as part of their induction.
- All staff are made aware of their individual responsibilities relating to the safeguarding of children within the context of e-Safety and know what to do in the event of misuse of technology by any member of the school community (see enclosed flowchart).
- All staff are encouraged to incorporate e-Safety activities and awareness within their curriculum areas.

Managing the School e-Safety Messages

- We endeavour to embed e-Safety messages across the curriculum whenever the internet and/or related technologies are used.
- E-Safety posters will be prominently displayed.
- Information will be sent to parents at the start of each school year regarding this policy.

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 Headteacher or Computing Lead. Additionally, all security breaches, lost/stolen equipment or data (including remote access Secure ID tokens and PINs), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be also be reported to the Computing Lead.

Misuse and Infringements

Complaints

Complaints and/or issues relating to e-Safety should be made to the Computing Lead or Headteacher. Incidents should be logged.

Inappropriate Material

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the Computing Lead.
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the Computing Lead, depending on the seriousness of the offence; investigation by the Headteacher/SEEAT Board, immediate suspension, possibly leading to dismissal and involvement of Police for very serious offences (see flowchart).
- Users are made aware of sanctions relating to the misuse or misconduct by the Headteacher, including disciplinary warnings, and ultimately, dismissal.
Essex flowchart to assist Headteachers, Senior Leaders and e-Safety Coordinators in the decision making process related to an illegal e-safety incident

Following an e-safety incident a decision will have to be made quickly as to whether the incident involved any illegal activity

Has illegal activity taken place?

YES

NO

Still unsure?
For further advice ECC ISIS helpdesk on 01245 431851 or Essex Police on 0300 333 4444

Users must be aware that if they find something unpleasant or frightening they should switch off their screen or close the laptop and talk to a member of staff

Examples of illegal activity would include:
- Downloading abusive images
- Passing child pornography to others
- Inciting racist or religious hatred
- Extreme cases of cyberbullying

If a member of staff has:
1. Behaved in a way that has, or may have, harmed a child
2. Possibly committed a criminal offence
3. Behaved towards a child in a way that indicates that s/he may be unsuitable to work with children Contact LADO on 01245 436744

- Review evidence and determine whether the incident was accidental or deliberate
- Decide upon the appropriate course of action
- Follow school disciplinary procedures (if deliberate) and contact Schools HR on 01245 436120 or your schools Link Officer

If a pupil is involved contact Social Care Direct to make an emergency referral on 0845 603 7634
- If it involves a member of staff contact the LADO on 01245 436744

Users must be aware that if they find something unpleasant or frightening they should switch off their screen or close the laptop and talk to a member of staff

YES

NO

Has illegal activity taken place?

Go to next flowchart which outlines the process for non-illegal incidents

✓ Inform Essex Police and Essex County Council
✓ Follow the advice given by the Police, or
✓ Confiscate the device and if related to the school network disable user account
✓ Save ALL evidence but DO NOT view or copy. Let the Police review the evidence
✓ If a pupil is involved contact Social Care Direct to make an emergency referral on 0845 603 7634
✓ If it involves a member of staff contact the LADO on 01245 436744

Still unsure?
For further advice ECC ISIS helpdesk on 01245 431851 or Essex Police on 0300 333 4444

Incident types could be:
- Using another persons user name or password
- Accessing websites which are against the schools policy e.g. gaming
- Using a mobile phone to take video during a lesson
- Using technology to upset or bully

Review incident to decide if other pupils were involved
- Decide appropriate sanctions
- Inform Parent/Carer if serious or persistent incident
- If serious, consider informing the Duty Safeguarding Officer as the child instigator could be at risk

The Head of School/e-Safety Co-ordinator should:
- Record the incident in the e-safety log
- Keep any evidence
- Support the pupil by one or more of the following:
  - Class Teacher
  - e-Safety Co-ordinator
  - Head of School/Senior Leader
  - Designated Child Protection Officer
  - School PCSO
  - Inform Parent/carer as appropriate

If the child is at risk contact Social Care Direct to make an emergency referral on 0845 603 7634
Internet Access

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 the Essex Grid for Learning (EGfL) is logged and the logs are randomly but regularly monitored. Whenever any inappropriate use is detected it will be followed up.

Managing the Internet

- Staff will preview any recommended sites before use.
- Where children use search engines to search for images the activity is supervised, and the school’s firewall will make this a safe activity.
- 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 its intended restricted audience.
- Don’t reveal names of colleagues, customers or clients or any other confidential information acquired through your job on any social networking site or blog.
- On-line gambling or gaming is not allowed.

It is at the Headteacher’s discretion what internet activities are permissible for staff and pupils and how this is disseminated.

Infrastructure

- Essex County Council has a monitoring solution via the Essex Grid for Learning where web-based activity is monitored and recorded
- School internet access is controlled through Exa Education Internet and filtering for schools. For further information relating to filtering please go to
  https://exa.net.uk/education/
- Staff and pupils are aware that school-based email and internet activity can be monitored and explored further if required.
- The school uses management control tools for controlling and monitoring workstations.
• If staff or pupils discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the E-safety Lead or teacher as appropriate.

• 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 manager’s, to install or maintain virus protection on personal systems.

• Pupils and staff are not permitted to download programs or files on school-based technologies without seeking prior permission from the Computing Lead.

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

Managing Other Web 2 Technologies

Web 2, 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. We understand that the legal age for access to sites such as Facebook is 13. Nevertheless, we acknowledge that some children will be accessing these sites earlier than that and will require guidance.

• At present, the school endeavors to deny access to social networking sites to pupils within school.

• All pupils are advised to be cautious about the information given by others on sites, 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 sites 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 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 pupils are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.

• Pupils are encouraged to be wary about publishing specific and detailed private thoughts online.

• Our pupils are asked to report any incidents of bullying to the school.

Parental Involvement

We believe that it is essential for parents/carers to be fully involved with promoting e-Safety both in and outside of school and also to be aware of their responsibilities. We regularly consult and discuss 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 at the stage that their child is inducted into school (part of the induction pack).

- 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 images, sounds or text that could upset or offend any member of the school community

- The school disseminates information to parents relating to e-Safety where appropriate in the form of:
  - Information and celebration evenings
  - Posters
  - Website
  - Newsletter items

**Passwords and Password Security**

**Passwords**

- 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 pupils who have left the School are removed from the system within one month.

**If you think your password may have been compromised or someone else has become aware of your password report this to the Computing Lead.**

**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 secret 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 e-safety Policy and Data Security

• Users are provided with an individual network, email, Learning Platform and Management Information System (where appropriate) login username.

• Pupils are not allowed to deliberately access online 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 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.

• In our school, all ICT password policies are the responsibility of the Headteacher, and all staff and pupils are expected to comply with the policies at all times

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 unauthorised access

• Regularly change generic passwords to avoid unauthorised access (Microsoft© advise every 42 days)

Further advice available [http://www.itgovernance.co.uk/](http://www.itgovernance.co.uk/)

Personal or Sensitive Information

Protecting Personal, Sensitive, Confidential and Classified Information

• Ensure that any School information accessed from your own PC or removable media equipment is kept secure

• Ensure you lock your screen before moving away from your computer during your normal working day to prevent unauthorised access

• Ensure the accuracy of any personal, sensitive, confidential and classified information you disclose or share with others

• Ensure that personal, sensitive, confidential or classified information is not disclosed to any unauthorised person

• Ensure the security of any personal, sensitive, confidential and classified information contained in documents you e-mail, fax, copy, scan or print. This is particularly important when shared mopiers (multi-function print, fax, scan and copiers) are used and when access is from a non-school environment.

• Only download personal data from systems if expressly authorised to do so by your manager.

• You must not post on the internet personal, sensitive, confidential, or classified information, or
disseminate such information in any way that may compromise its intended restricted audience.

- Keep your screen display out of direct view of any third parties when you are accessing personal, sensitive, confidential or classified information.

- Ensure hard copies of data are securely stored and disposed of after use in accordance with the document labeling.

**Storing/Transferring Personal, Sensitive, Confidential or Classified Information Using Removable Media**

- Ensure removable media is purchased with encryption.

- Store all removable media securely.

- Securely dispose of removable media that may hold personal data.

- Encrypt all files containing personal, sensitive, confidential or classified data.

- Ensure hard drives from machines no longer in service are removed and stored securely or wiped clean.

**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. ECC guidance can be found: [http://esi.essexcc.gov.uk/vip8/si/esi/content/binaries/documents/Service_Areas/Governance/Information_Governance_doc_February_2010_2.doc](http://esi.essexcc.gov.uk/vip8/si/esi/content/binaries/documents/Service_Areas/Governance/Information_Governance_doc_February_2010_2.doc)

- 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 Headteacher, 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 others, this includes when on school 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 pupil’s device

**Publishing Pupils’ 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;
• 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;
• permission for general media appearances, e.g. local/national media/press releases sent to the press highlighting an activity (sent using traditional methods or electronically) will be sought separately.

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. 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.

Only the Web Manager has authority to upload to the school website.

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 Headteacher
• Rights of access to this material are restricted to the teaching staff and pupils within the confines of the school network/ Learning Platform
• The ICT technician has the responsibility of deleting the images when they are no longer required, or the pupil has left the school

Webcams and CCTV

• The school uses CCTV for security and safety. The only people with access to this are the Site and Office Managers.
• We do not use publicly accessible webcams in school.
• Webcams in school are only ever used for specific learning purposes, e.g., monitoring hens’ eggs and never using images of children or adults.
• Misuse of the webcam by any member of the school community will result in sanctions (as listed under the ‘inappropriate materials’ section of this document).
School ICT Equipment including Portable & Mobile ICT Equipment & Removable Media

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

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

Portable & Mobile ICT Equipment

This section covers such items as laptops, PDAs 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’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 staff, fully licensed and only carried out by your ICT staff.

• 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, PDAs, 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 pupil or parent/carer using their personal device.

• Pupils in Years 5 and 6 are allowed to bring personal mobile devices/phones to school but must not use them for personal purposes within lesson time. The phones will be kept by the office staff during the day as their use is solely for contacting parents after school. Parents will register their children’s phones with the school and sign a mobile phone user agreement.

• 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 the 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

- Newly installed servers holding personal data should be encrypted, therefore password protecting data. SIMs Database Servers installed by SITSS since April 2009 are supplied with encryption software.
- Always keep servers in a locked and secure environment.
- Limit access rights to ensure the integrity of the standard build.
- Always password protect and lock the server.
- Existing servers should have security software installed appropriate to the machine’s specification.
- Back up tapes should be encrypted by appropriate software.
- Data must be backed up regularly.
- Back up tapes/discs must be securely stored in a fireproof container.
- Back up media stored off-site must be secure.
- Remote back-ups should be automatically securely encrypted.
- Regular updates of anti-virus and anti-spyware should be applied.
- Records should be kept of when and which patches have been applied.
- Ensure that web browsers and other web-based applications are operated at a minimum of 128 BIT cipher strength.
Smile and Stay Safe Poster

e-Safety guidelines (or similar) to be displayed throughout the school

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’.

Let 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.
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 or ECC 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, racist 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 Equality Act 2010).
- 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.
- It is essential that any hard drives which may have held personal or confidential data are ‘scrubbed’ in a way that means the data can no longer be read. It is not sufficient to simply delete the files or reformat the hard drive. Whoever you appoint to dispose of the equipment must provide a written guarantee that they will irretrievably destroy the data by multiple over writing of the data.

Telephone Services

- You may make or receive personal telephone calls provided:
  1. They are infrequent, kept as brief as possible and do not cause annoyance to others
  2. They are not for profit or to premium rate services
  3. They conform to this and other relevant SEEAT and school policies.
- School telephones are provided specifically for school business purposes and personal usage is a
privilege that will be withdrawn if abused.

- Be aware that the laws of slander apply to telephone calls. Whilst a telephone call may seem to have a temporary and private existence it still qualifies as admissible evidence in slander law cases.

- Ensure that your incoming telephone calls can be handled at all times

- Follow the appropriate procedures in the event of receiving a telephone call containing a bomb threat. These procedures should be made readily available throughout your office. If you do not have a copy, please ask your line manager.

**Writing and Reviewing this Policy**

**Staff and Pupil Involvement in Policy Creation**

Staff have been involved in making/ reviewing the Policy for ICT Acceptable Use through staff meetings.

**Review Procedure**

There will be an on-going opportunity for staff to discuss with the Computing Lead any issue of e-Safety that concerns them.

There will be an on-going opportunity for staff to discuss with the SIRO/AIO any issue of data security that concerns them.

This policy will be reviewed every 2 years 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.

<table>
<thead>
<tr>
<th>Reviewed during</th>
<th>Spring Term 2019</th>
</tr>
</thead>
<tbody>
<tr>
<td>Approved by Governing Body</td>
<td></td>
</tr>
<tr>
<td>Next review</td>
<td>Spring Term 2021</td>
</tr>
</tbody>
</table>

Signed: [Signature]

Date: January 2019

Chair of Governors: Sonia Worthington