E-safety Policy Market Field School School E-safety policy

Writing and reviewing the E-safety Policy

The E-safety Policy is part of the School Monitoring and review Schedule and relates to other policies including those for computing education, anti-bullying and for child protection.

The school has appointed the Assistant Headteacher for Key Stage 3 and 4 as its E-safety coordinator.

The E-safety Policy and its implementation will be reviewed annually

Teaching and learning:

Why internet and digital communications are important

The internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality internet access as part of their learning experience.

Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

The school internet access is provided by Essex County Council through a regional broadband contract, which includes filtering appropriate to the age of pupils.

Pupils will be taught what internet use is acceptable and what is not and given clear objectives for internet use.

Pupils will be educated in the safe, effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.

Pupils will be shown how to publish and present information appropriately to a wider audience.

Pupils will be taught how to evaluate internet content

The school will seek to ensure that the use of internet derived materials by staff and by pupils complies with copyright law.

Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Pupils will be taught how to report unpleasant internet content e.g. using the CEOP Report Abuse icon or Hector Protector. For pupils whose parents lack economic or cultural educational resources, the school should build digital skills and resilience acknowledging the lack of experience and internet at home.

Managing internet Access Information system security

- School ICT systems security will be reviewed regularly.
- Virus protection will be updated regularly.
- Security strategies will be discussed with the Local Authority.

E-mail

- Pupils and staff may only use approved e-mail accounts on the school system (where they are set up) for matters related to school.
- Pupils/parents/carers must immediately tell a teacher if they receive offensive e-mails linked to school.
- Staff to pupil/parent/carer email communication must only take place via a school email address or from within Dojo and will be monitored except when the pupil is known to the member of staff in a capacity other than through school e.g. if a member of staff has a child at the school they may have other parents' details in order to arrange play dates.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- The forwarding of chain letters is not permitted.
- Cc/Bc or inform head teacher of any e-mail deemed sensitive.

Published content and the school website

The contact details on the website should be the school address, e-mail and telephone number.

The Deputy Headteacher, School Business Manager support and Finance Assistant will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupils' images and work

Photographs that include pupils will be selected carefully.

Pupils' full names will be avoided on the website or Dojo as appropriate, included in blogs, forums or wikis, particularly in association with photographs.

Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.

Parents should be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories.

Social networking and personal publishing on the class Dojo app

The school will educate pupils in the safe use of social networking sites through the use of the Dojo app e.g. use of usernames, passwords etc.

Pupils will be advised never to give out personal details of any kind which may identify them or their location.

Pupils/parents/carers must not place personal photos on any social network space provided on the Dojo app.

Pupils/parents/carers will be advised that the use of social network spaces outside school brings a range of opportunities; however it does present dangers for pupils.

Social Networking sites

If you use Facebook, Twitter or other social networking sites you must not share anything which may bring the school into disrepute. Ensure that your privacy settings are locked down and remember that these settings need to be checked every time the site owners update the site.

Managing filtering

The school will work in partnership with Essex County Council to ensure systems to protect pupils are reviewed and improved.

If staff or pupils come across unsuitable on-line materials the site must be reported to the class teacher (pupils) or the Headteacher (staff) immediately.

School Leaders will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Managing emerging technologies

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

Handheld technologies, including games and mobile phones, often have internet access which may not include filtering. Care will be taken with their use within the school.

The appropriate use of learning platforms will be discussed as the technology becomes available within the school.

Mobile Device guidance

Market Field School has a responsibility to ensure that all data stored on its computer systems is appropriate to the needs of the organisation, is securely held and complies with the requirements of the Data Protection Act 1998. The use of portable computer devices increases the risks associated with the secure storage of data. The guidance relating to the use of school owned laptop computers and data stored on school-owned or personal removable media (e.g. flash drives/memory sticks, external hard drives) can be found in Appendix A at the back of this policy.

General use of mobile phones

Mobile phones and personally-owned devices will not be used in any way during lessons or formal school time. They should be switched off or silent at all times.

Mobile phones and personally-owned mobile devices brought in to school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally-owned mobile phones or mobile devices.

Mobile phones will not be used during lessons or formal school time unless as part of an approved and directed curriculum-based activity with consent from the Head Teacher.

No images or videos should be taken on mobile phones or personally-owned mobile devices in school.

Staff use of personal devices

Staff are not permitted to use their own mobile phones or devices for contacting children, young people or their families in a professional capacity within or outside of the setting.

Mobile Phones and personally-owned devices will be switched off or switched to 'silent' mode and kept out of sight of children. Mobile phones or devices will not be used during teaching periods unless permission has been granted by the Head Teacher in emergency circumstances.

If members of staff have an educational reason to allow children to use mobile phones or a personal device as part of an educational activity then it will only take place when approved by the Head Teacher.

Staff should not use personal devices such as mobile phones or cameras to take photos or videos of pupils and will only use work provided equipment for this purpose.

If a member of staff breaches the school policy then disciplinary action will be taken as appropriate.

Staff use of mobile phones during the school day should be limited.

Staff should ensure that their phones are protected with PIN codes in case of loss or theft.

Staff should never contact parents/carers or students from their personal mobile phone, or give their mobile phone number to students/parents/carers – except when the parent /carer is a personal friend or a family member and is known to them in a capacity other that through school. If a member of staff needs to make telephone contact with a parent/carer, a school telephone should be used.

Staff should never store parents/pupils/carers telephone numbers on their mobile phone, as this allows the possibility of inappropriate contact. (See exception in previous bullet point)

Staff should never send to, or accept from anyone, texts or images that could be viewed as inappropriate.

Protecting personal data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

Policy Decisions authorising internet access

All staff must read and sign the Staff Behaviour Policy before using any school ICT resource.

The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.

Access to the internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.

Parents will be asked to sign and return a consent form.

Assessing risks

The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor ECC can accept liability for the material accessed, or any consequences of internet access. The school will monitor ICT use to establish if the E-safety policy is adequate and that the implementation of the E-safety policy is appropriate and effective.

Handling E-safety complaints

Complaints of internet misuse will be dealt with by a senior member of staff.

Any complaint about staff misuse must be referred to the Head Teacher (or Chair of Trustees if it relates to Head Teacher).

Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

Pupils and parents will be informed of the complaints procedure.

Community use of the internet

All use of the school internet connection by community and other organisations shall be in accordance with the school E-safety policy.

Communications Policy - **Introducing the E-safety policy to pupils**

Appropriate elements of the E-safety policy will be shared with pupils

E-safety rules will be posted in all networked rooms.

Pupils will be informed that network and internet use will be monitored.

Curriculum opportunities to gain awareness of E-safety issues and how best to deal with them will be provided for pupils.

This should be addressed each year as students become more mature and the nature of newer risks can be identified.

Staff and the E-safety policy

All staff will be given access to the School E-safety Policy and its importance explained.

All staff will sign to acknowledge that they have read and understood the E-safety policy and agree to work within the agreed guidelines.

Staff should be aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

Staff that manage filtering systems or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues.

Enlisting parents' support

Parents' and carers' attention will be drawn to the School E-safety Policy in newsletters and on the school website.

The school will ask all new parents/carers to sign the parent/carer pupil agreement when they register their child with the school.

Parents should be offered E-safety training regularly with a focus on education and having an overview of tools to allow them to take control whilst not undermining trust.

Often children do not wish to be constantly online but often lack sufficient alternatives for play, travel interaction and exploration. Parents should be encouraged, where possible to interact with their children on the internet as well as provide other opportunities for learning and recreation.

Appendix A Laptop and Removable Storage Advice

For the purpose of this policy the term “laptop” is used to describe any portable computer device including laptops, notebooks, tablet PCs, cameras, flash drives, on which school data may be stored. Your laptop is a valuable asset and an essential business tool. It needs to be protected, as does the information it stores. Remember that the laptop and the information that it contains could be valuable to thieves. By following the simple security measures listed below, you can help protect yourself and your laptop.

Teacher/ Staff Responsibilities

Teachers/ members of staff must take personal responsibility for the security of the equipment, software and data in their care and abide by the following:

- Laptops in cars must be stored out of sight (e.g. in covered boot). Laptops should never be left in a vehicle for prolonged periods of time or overnight.
- Always lock your laptop away when it is not in use in school.
- Un-authorised or unlicensed software must not be loaded on to the laptop.
- Ensure the laptop is not used by un-authorised persons.
- Take all reasonable steps to ensure that the laptop is not damaged through misuse.
- When travelling, laptops should not be left unattended in public places.
- Remain particularly vigilant when using your laptop and try to refrain from using it in public places (e.g. library, railway station).
- Return the laptop to school for regular health checks or when requested and ensure that the laptop antivirus software is updated by the school ICT technician (automatic updates to be reviewed by the Technician at least annually).
- Ensuring that the protection settings are left as set up by the technician (E.g. that Windows Firewall always runs, passwords are in place).
- Passwords should be kept safe. Update your passwords regularly and don’t let others use them.
- Return the laptop before leaving the employment of the school.
- Report any possible security breaches (eg. laptop stolen or misplaced) to the Head Teacher immediately.
- Ensure that the school office has noted any serial numbers for the equipment and asset tags have been created, where necessary.
- Back up your files regularly and store them securely.
- Do not allow family or friends to use your laptop, as there is a risk that school information could be compromised.

- Wherever possible, when storing data for work purposes, store the data on the encrypted drive supplied by the school. If you are attacked, don’t risk your own safety. Hand over the laptop. It can be replaced but you can’t.