The Mead Infant and Nursery School

E-Safety and IT Acceptable Use Policy

Proud to Belong

This Policy was adopted by The Governing Body and is reviewed annually. Last reviewed in Autumn Term 2019.

Reviewed by: T Creasey

Next Review: Autumn term 2021

The Mead Infant and Nursery School
E-safety and IT Acceptable Use Policy

E-safety is part of the school's safeguarding responsibilities. This policy also relates to other policies including those for Behaviour, Safeguarding, Anti-bullying, GDPR/Data Protection and School Laptop usage.

The Mead Infant and Nursery School is committed to ensuring that everyone in school is able to operate with safety and confidence whenever and wherever they use the Internet or mobile technologies.

What is e-Safety?

E-Safety encompasses internet technologies and electronic communications such as mobile phones as well as collaboration tools and personal publishing. It highlights the need to educate children about benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

Using this policy

- The school has an e-safety co-ordinator (Caroline Stahlecker)
- The e-safety policy has been written by the school, building on best practice and government guidance. It has been agreed by senior management and approved by Governors.
- This e-safety policy was revised by: T Creasey
- This e-safety policy and its implementation will be reviewed annually. The next review is due on: Autumn 2021
- This e-safety policy covers the use of all technology which can access the school network and the internet or which facilitates electronic communication from school to beyond the bounds of the school site. This includes but is not limited to workstations, laptops, mobile phones, tablets and hand held games consoles used on the school site.
- This e-safety policy recognises that there are differences between the use of technology as a private individual and as a member of staff/pupil.

Managing access and security

The school will provide managed internet access to its staff and pupils in order to help pupils to learn how to assess and manage risk, to gain the knowledge and understanding to keep themselves safe when using the internet and to bridge the gap between school IT systems and the more open systems outside school

- The school will use a recognised internet service provider or regional broadband consortium – this is currently Talk Straight.
- The school will ensure that all internet access has age appropriate filtering provided by a recognised filtering system (Lightspeed Systems) which is regularly checked to ensure that it is working, effective and reasonable.
- The school will ensure that its networks have virus and anti-spam protection (Sophos).

- Access to school networks will be controlled by personal passwords. There are automatic prompts set up to ensure that these are up-dated periodically.
- Systems will be in place to ensure that internet use can be monitored and a log of any incidents will be kept to help to identify patterns of behaviour and to inform e-safety policy.
- The security of school IT systems will be reviewed regularly.
- **All staff that manage filtering systems or monitor IT use will be supervised by senior management and have clear procedures for reporting issues.**
- The school will ensure that access to the internet via school equipment for anyone not employed by the school is filtered and monitored.
- Staff will not install any software on to school computers without authorisation given by the Headteacher, Computing Co-ordinator (Caroline Stahlecker) or ICT Technician (S. Hutton).
- The school assesses the risks to ensure the safe and secure use of personal data within the school

Internet Use

- It is vitally important that staff are careful about content that they search out or download. Every time a page is viewed on the internet, it is possible to trace that visit back to the school computer. This means that it is possible to tell if a school computer was being used to look at inappropriate web pages.
- The school will provide an age-appropriate e-safety curriculum that teaches pupils how to stay safe, how to protect themselves from harm and how to take responsibility for their own and others' safety.
- All communication between staff and pupils or families will take place using school equipment and/or school accounts.
- Pupils will be taught not to give out personal details or information which may identify them or their location.

E-mail

- Pupils and staff may only use approved e-mail accounts on the school IT systems.
- All incoming and outgoing emails can be read by our web host manager. This is not intended to infringe on staff privacy, but the internet is a very public way of communicating and like all companies, management reserves the right to ensure that the name of the school is not brought into disrepute.
- Great care must be taken when sending emails containing confidential information; only initials will be used to identify children unless the email is being sent via 'Egress' secure system. To send an email in this way please see Sue Hortop (School Business Manager).
- Incoming e-mail should be treated as suspicious and attachments **never** opened unless the author is known.

Published content e.g. school web site, school social media accounts

- The contact details will be the school address, email and telephone number. Staff or pupils' personal information will not be published.
- The Headteacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupils' images and work

- Written permission will be obtained from parents or carers before photographs or names of pupils are published on the school web site or any school run social media as set out in Surrey Safeguarding Children Board Guidance on using images of children. http://www.surreycc.gov.uk/

Social Networking

- The following guidance, will safeguard adults from allegations and protect an individual's privacy as well as safeguard vulnerable groups. Failure to comply may result in disciplinary action
- Staff and volunteers should be aware of the impact of their personal use of social networking sites upon their professional position. In practice, anything posted on the Internet will be there forever and is no longer in the control of the individual who created the post. Even is something is removed from the Internet, it may have already been duplicated by a 'web crawler' and so will always be there. Current and future employers and service users may see this. Staff are encouraged to keep all professional work completely separate from their private life.
- Staff must be aware of their responsibilities to the school when using social media at all times, even outside of working hours. It is important to maintain their status as a professional and therefore the school would urge staff to think twice before fostering online friendships with parents. Disciplinary action could result if the school is brought into disrepute.
- Staff must not post anything onto social networking sites such as 'Facebook' that could be construed to have any impact on the school's reputation
- Staff must not post photos related to the setting on any internet site including children, colleagues or parents
- Staff must not post anything onto social networking sites that would offend any other member of staff or parent of the school
- The school will control access to social networking sites, and consider how to educate pupils in their safe use. This control may not mean blocking every site; it may mean monitoring and educating students in their use.
- Use of video services such as Skype, Google Hangouts and FaceTime will be monitored by staff. Pupils must ask permission from a member of staff before making or answering a video call.
- Staff and pupils should ensure that their online activity, both in school and out takes into account the feelings of others and is appropriate for their situation as a member of the school community.

'Safeguard yourself' Guidelines

Social networking sites such as Facebook have a range of privacy settings that are often set up to 'expose' someone's details to anyone. When 'open' anyone can find a person from a search of the social networking site or even from a Google search. Therefore, it is important to change the setting to 'just friends' so that a person's details, comments, photographs can only be seen by invited friends. Please read the following guidelines to further 'Safeguard Yourself'.

- Have a neutral picture of yourself as your profile image
- Do not post embarrassing material or comments that may call into question your employment status
- Do not accept friendship requests unless you know the person or want to accept them - be prepared for being bombarded with friendship requests from people you do not know
- Do not make friendship requests with service users
- Choose your social networking friends carefully and ask about their privacy controls
- Do not accept friendship requests on social networking or messaging sites from the children, young people (or their parents) or service users that you work with. For those working with young people remember that ex pupils may still have friends that you may have contact with through your work
- Exercise caution. For example, if you write on a friends 'wall' on Facebook all of their friends can see your comment even if they are not your friend
- There is a separate privacy setting for Facebook groups and networks. You may have your own profile set to private, however, when joining a group or a network please be aware that everyone in that group or network is able to see your profile
- If you have younger friends or family members on your social networking groups who are friends with children, young people (or their parents) or service users that you work with, be aware that posts you write will be visible to them
- Do not use your personal or professional details (email or telephone) as part of your profile
- If you or a friend are tagged in an online photo album (Facebook, flickr) the whole photo album may be visible to their friends, your friends and anyone else tagged in the photo album
- You do not have to be friends with anyone to be tagged in their photo album, if you are tagged in a photo you can remove the tag but not the photo
- You should be aware of the privacy settings on photo sharing websites
- Your friends may take and post photos that you may not be happy about. You need to speak to them first to request that it is removed rather than contacting the web provider. If you are over the age of 18, the website will only look into issues that contravene their terms and conditions
- Do not use your personal profile in any way for official business. If you are going to be a friend of your organisations official social networking group, ensure you have a separate professional profile

If staff have difficulty in implementing any of this guidance they must speak to the Headteacher.

Use of personal devices including mobile phones

- Mobile phones and personally-owned devices may not be used during lesson time. They should be switched off or on silent and left in a safe place. They should be out of sight during lessons, assemblies and whilst moving throughout the school
- It is not appropriate at any time to take/store photos or videos of children during the school day on a personal device
- Staff are not permitted to use their own mobile phone to call or send pictures/videos to pupils or parents at any time and should only use school provided equipment for this purpose

- Staff should never send, or accept from anyone, texts or images that could be viewed as inappropriate
- If a member of staff suspects a message, text or similar may contain inappropriate content then the Designated Safeguarding Lead should be informed
- The school cannot be held responsible for the loss or damage of any personal devices used in school or for school business.

Use of portable storage devices

- Always run a virus scan on a USB stick before opening on a school computer

Possession of Images

- There are no circumstances that will justify adults possessing indecent images of children. Adults who access and possess links to such websites will be viewed as a significant and potential threat to children. Accessing, making and storing indecent images of children is illegal. This will lead to criminal investigation and the individual being barred from working with children, if proven.
- Adults should not use equipment belonging to the school to access adult pornography, neither should personal equipment containing these images or links to them be brought into school. This will raise serious concerns about the suitability of the adult to continue to work with children
- Adults should ensure that children are not exposed to any inappropriate images or web links.
- Passwords should be kept confidential.

Policy Decisions

Authorising access

- All staff (including teaching assistants, support staff, office staff, lunchtime learning assistants, student teachers, work experience trainees, ICT technicians and governors) must confirm that they have read and sign this policy before accessing the school IT systems (a copy of the policy can be obtained from the school bursar).
- The school will maintain a current record of all staff and pupils who are granted access to school IT systems.
- Access to the internet will be by adult demonstration with supervised access to specific, approved on-line materials.
- People not employed by the school must read and sign a Guest AUP before being given access to the internet via school equipment.
- Parents will be asked to sign and return a consent form to allow use of technology by their pupil.

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 SCC can accept liability for the material accessed, or any consequences of internet access.

Handling e-safety complaints

- Complaints of internet misuse will be dealt according to the school behaviour policy.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of consequences and sanctions for pupils misusing the internet and this will be in line with the school's behavior policy.

Community use of the internet

- Members of the community and other organisations using the school internet connection will have signed a guest AUP so it is expected that their use will be in accordance with the school e-safety policy.

Communication of the Policy

To staff

- All staff will be shown where to access this e-safety policy and its importance explained.
- All staff will receive e-safety training

To parents

- The school will ask all new parents to sign the parent /pupil agreement when they register their child with the school.
- Parents' and carers' attention will be drawn to the School e-safety Policy in newsletters, and on the school web site.
- Parents will be offered e-safety training