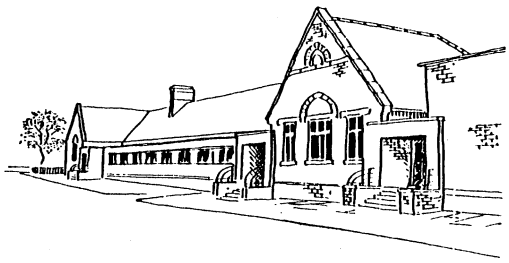
Mundella Primary School Policies



Acceptable Use Policy

Date Created/Updated: July 2017

Created/Updated by: Headteacher, SBM, ICT subject co-ordinator

Date to be Reviewed: July 2019

Primary school pupils should always be carefully supervised when using school ICT systems, particularly when accessing the Internet.

It's important that the class teacher explains rules for e-safety to the class, so that pupils understand what they mean and why they are important in keeping everyone safe. These will be displayed prominently in places where pupils will access the Internet, for instance in ICT suites or next to classroom-based computers.
Explain to pupils that the school checks what they have done on the school ICT systems regularly, including which websites they visit. Also explain what might happen if they don't follow the rules, for instance parents may be informed.

However, it is important that pupils know they will not be blamed for accidental incidents. For example, if pupils accidentally access an inappropriate website, they need to be confident to report this to an adult without fear of blame.

See eSafety AUP KS1 - Sept 17 and eSafety AUP KS2 - Sept 17 for the agreements that children need to sign.

AUP for all staff and adults in school

The following statements are designed to be used with staff and other adults in school to outline what is, and is not, acceptable and responsible behaviour whilst using Internet-based resources in school.
Staff are expected to take care to use the ICT systems in school in a responsible manner, maintaining the integrity of the systems and the security of personal data. They should also promote the school eSafety policy and a culture of safe use of technology to pupils by reinforcing the pupil AUP and modelling good practices in lessons.
It's important that staff take care to ensure their personal use of technologies outside of school do not come into conflict with their professional role as a teacher, or potentially put themselves at risk through pupils initiating contact with them online.
Staff need to be aware that their use of the school ICT systems is being monitored and can be checked at any time, and be aware of what disciplinary action may be taken against them in the event of a deliberate infringement.

Staff should sign their acceptance of the end-user AUP and schools should record this centrally. The end-user AUP should be discussed in a staff meeting so that everyone is aware of its contents, and reviewed alongside staff regularly.

These statements are designed to ensure staff and other adults in school are aware of their professional responsibilities when using the ICT systems provided. All staff should follow the guidelines at all times. You are responsible for your behaviour and actions when accessing the Internet at school, whether on your own or school equipment, and when using school ICT equipment at other locations such as your home.

- Any use of school ICT systems will be for professional purposes as agreed by the school senior management team
- Usernames, passwords and other logon details should be kept secure and not revealed to anyone else. Care should be taken to ensure you logout when not actively using the ICT systems. You should not allow an unauthorised person to access the school ICT systems, e.g by logging in for them. On the occasions when a parent may need to use your computer (eg supporting a parent in completing a secondary school transfer form) you should remain with them at all times
- Ensure that wherever possible only school equipment is used to take photographs of children. This means using a school i-pad when children are in school and using the school mobile phone during residential visits. On occasions staff may use their own personal equipment to take photos on educational visits. The photos must be deleted on return from the visit.
- Photographs of children can only appear with forenames.
- Any photographs taken on i-pads or any mobile phones should be deleted.
- If you leave your computer unattended, it should be locked to prevent other people accessing your data.
- Any online activity should not harass, harm, offend or insult other users.
- You will not search for, download, upload or forward any content that is illegal, or that could be considered offensive by another user. If you accidentally encounter such material you should follow your school's procedure and report this immediately.
- You should not download or install any hardware or software without permission. If you have responsibility for installing software you should be confident it is adequately licensed and appropriate for educational use.
- Ensure that any files on removable media (e.g. USB drives, CDs) are free from viruses and other malware before use and that such devices are not used for carrying sensitive data or details of pupils, parents or other users without suitable security and without permission from the Headteacher.
- Any electronic communications should be related to schoolwork only, and should be through school e-mail addresses or other school systems e.g. learning platforms. It is not acceptable to contact pupils using personal equipment or personal contact details, including your own mobile phone or through your personal social network profiles.
- Any online activity, including messages sent and posts made on websites, and including activity outside of school, should not bring your professional role or the name of the school into disrepute. You should check to ensure your privacy settings on such sites as Facebook.

- Any still or video images of pupils and staff should be for professional purposes only. They should be taken on school equipment, and stored and used onsite. Such images should not be taken off-site without permission and valid reason.
- You will not give out your personal details, or the personal details of other users, to pupils or parents or on the Internet. In particular you should ensure your home address, personal telephone numbers and email accounts are not shared with children, young people or parents. (There are, however, staff who are members of the local community who have personal friends who are parents. These staff members may well have given their numbers to these friends. Be aware though of the need to be discreet and professional at all times.)
- You should ensure that any personal or sensitive information you use or access (e.g. SIMS data, assessment data) is kept secure and used appropriately.
- Personal or sensitive information should only be taken off-site if agreed with the Headteacher, and steps should be taken to ensure such data is secure.
- You should respect intellectual property and ownership of online resources you use in your professional context, and acknowledge such sources if used.
- You should support and promote the school eSafety Policy, and promote and model safe and responsible behaviour to pupils when using ICT to support learning and teaching.
- No photos of staff events (eg end of term celebrations etc) should be posted on any web based site (eg Facebook; You Tube etc.)

Finally:

- You understand that your files, communications and Internet activity may be monitored and checked at all times to protect your own and others' safety, and action may be taken if deemed necessary to safeguard yourself or others. If you do not follow all statements in this AUP and in other school policies you may be subject to disciplinary action in line with the school's established disciplinary procedures.

Signed ……. Name ……

Date……