Annemount
Nursery and Pre-preparatory School

Annemount School

ICT Acceptable Use Policy for Staff

As a professional organisation with responsibility for young people's safeguarding it is important that all staff take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft. All members of staff have a responsibility to use the schools' computer systems in a professional, lawful, and ethical manner. To ensure that members of staff are fully aware of their professional responsibilities when using Information Communication Technology and the school systems, they are asked to read and sign acknowledgement of this Acceptable Use Policy.

- It should be understood that this Code of Practice is in place to protect staff from potential risk in their use of ICT in their everyday work.
- This Acceptable Use Policy should be read in conjunction with the schools Online Safety Policy and the Teacher and Staff Handbook.
- Teachers should be familiar with the school Safeguarding Policy.
- Pupils should only use laptops when logged in as 'Student'. Student user settings have appropriate restrictions.
- Teachers should closely monitor and scrutinise what their pupils are accessing on the iPads and laptops.
- When pupils are using the internet, it should be controlled by a teacher or adult.
- Pupils should be given a clearly defined focus for using the internet or email and taught skills and techniques to enable efficient and effective use of it.
- Software should not be downloaded from the internet (including screen savers, games etc.) or installed by anyone other than IT Support (VirtualITEducation), unless permission has been granted by the Head Teacher.
- You must be aware of what is on your screen and potentially viewed by pupils when accessing the internet using a 'teacher' log-in/user. Teachers must prepare internet searches prior to pupils' arrival and the start of a lesson.
- Under no circumstances must you open the internet to search for something when your Interactive Whiteboard is on and the children can see the screen.
- When using a search engine to research, the children should be taught to use **Kiddle** rather than Google. This is a child friendly search engine site.
- Staff are asked to complete a filtering check on their laptops annually and record and report the results.
- All sensitive data, such as children's details or reports, should be stored on a password protected storage device.
- The use of the internet to access any illegal sites or inappropriate material is a disciplinary offence.
- If offensive material is accessed accidentally, the website should be closed immediately and the incident reported to the Head Teacher and logged.
- Always ensure that when taking and /or publishing images of others, permission has been obtained in accordance with the school's policy on the use of digital/video images and a school camera has been used. Using personal equipment to record these images is not appropriate, unless you have permission to do so, and these photographs will not be shared on the internet or put on public display without permission.
- Teachers should understand that the school use of the internet on school premises should be for school use, e.g. accessing learning resources, educational websites, researching curriculum topics, use of email on school business. Teachers should not be accessing the internet for personal reasons.
- The school recognises that many staff will actively use social media such as Facebook, Instagram, X (previously Twitter), and other networking sites, blogging and messaging services. Staff must not post material (including text or images) which damages the reputation of the school or which causes concern about their suitability to work with children. Staff must recognise that it is not appropriate to discuss issues relating to children or other staff via these networks.

- The relationship the staff team has with parents and families of pupils is and must remain strictly professional. It is appropriate therefore for social media accounts held by staff to be private. It is not appropriate to “friend” parents or comment or send emojis to parent social media accounts, even if their accounts are public. It is important that this is understood and that there is no blurring of the boundaries or risk that your reputation or the reputation of the school could be compromised.
- It is entirely possible that there may be pupils of families who are high profile with very public profiles. It is particularly important in these instances that staff do not actively comment on these posts.
- Those who post material which could be considered as inappropriate could render themselves vulnerable to criticism or allegations of misconduct.
- It is never acceptable to accept a friendship request from pupils at the school, as in all cases, children of KS1 and EYFS age using such networks will be breaching terms and conditions of use of those networks.
- It is also extremely inadvisable to accept as friends ex-pupils who are still minors. If a parent of a pupil seeks to establish contact, the member of staff should exercise their professional judgement.
- Teachers should NOT use their personal phones during contact time with pupils or for taking photos of children, unless authorised by the Head Teacher.
- Mobile phones should not be used when teaching, unless authorised.
- The school does not allow the use of smart watches by teachers during the working day.
- For staff wishing to access internal school emails from home from personal devices, such as an iPhone, must first inform the office by email. Devices used must be password protected. In the event a personal device such as an iPhone is stolen or lost and the internal email system is compromised, the staff member must inform the school.