



Chertsey and Dorking Nursery Schools and Mole Valley Family Centre

E-SAFETY POLICY

AIMS

- To ensure all staff adopt safe practices in the use of the Internet and in the teaching of Internet use to children.
- To begin to educate children to be responsible and informed technology users.
- To ensure that e-safety is an integral part of our commitment to safeguarding children and relates to other policies.

SECURITY

- The Internet access provided includes filtering appropriate to the age of the children.
- The IT systems within are configured in order to restrict access to those who require it.
- The IT security system is protected by anti-virus protection and managed through IT support contracts, it is password controlled and ensures forced password changes.

INTERNET USE

- The Internet is a useful and necessary tool for staff.
- Children will not be allowed free access on the Internet.
- Parental permission is in place when images of children are used on websites or social media; children are not named. Children's full names will be avoided on any website or social media – see confidentiality policy about use of children's photographs on the Internet.
- Tapestry, an online learning journal is used. Images and observations, including names are an integral part of this system. Staff and parent access to Tapestry is password protected.
- Tablets are issued to staff to host Tapestry. They are PIN password protected.
- All staff are required to read and understand the e-Safety Policy, and adhere to it at all times.
- If staff come across unsuitable on-line materials, the site must be reported to the Headteacher immediately.
- It is a criminal offence to use a school IT system for a purpose not permitted by the organisation.
- Any complaint of staff misuse of the Internet must be referred to the Head.
- The IT information systems, internet and email may not be used for private purposes without specific permission from the Head.
- Use of school information systems, Internet and email may be monitored and recorded to ensure policy compliance.
- No member of staff should install any software or hardware without permission to any computers or tablets (including iPads and iPods)
- Memory sticks and other portable devices are not to be used by staff as they will contain data regarding children and families. All documents should be stored on the secure network or office 365 cloud only.
- Copyright and intellectual property rights should be respected at all times.

- Should any staff receive inappropriate material from a third party via email, this should be reported to the Head immediately.

Staff need to be aware in their private life that contents on social networking websites may be detrimental to their professional image.

The Staff Behaviour Policy and Staff Handbook give further information to employees regarding the safe use of IT, internet and e-safety.

Approved by the Governing Body: January 2020

To be reviewed by: January 2021

Relevant for:-

Centre: Yes	Nursery: Yes	Parents: Yes
--------------------	---------------------	---------------------