Chertsey and Dorking Nursery Schools

ONLINE SAFETY POLICY

AIMS

- To ensure all staff adopt safe practices in the use of the Internet and understand about acceptable use
- To begin to educate children and parents to be responsible and informed technology users
- To ensure that online safety is an integral part of our commitment to safeguarding children and relates to other policies
- To ensure that requirements from Keeping Children Safe in Education (2023) are reflected in our practice and policy

SECURITY

- Children across our organization do not have access to technology connected to the internet.
- 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 for those accessing the network.
- All staff are required to read and understand the Online Safety Policy at induction and when it is revised/updated. Staff are required to adhere to it at all times.
- Laptops and tablets are issued to some staff depending on their role. They are password protected.
- Any laptops or tablets used off site are not to be left unattended or in cars etc. See Staff Handbook for more details.
- There are filtering and monitoring systems in place for all users on the internet, these block inappropriate access to sites and will monitor any access to sites that are deemed to have inappropriate content.

SAFEGUARDING

- The lead DSLs on each site is responsible for ensuring that the filtering, monitoring and safeguarding processes are in place.
- Parental permission is in place when images of children are used on websites or social media; children are not named. Children's names are not used on any website or social media. We will rotate images of children on websites and displays linked to data retention.
- 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. Parents only have access to information about their own child and staff access is monitored at different levels depending on their role.
- Tablets and iPods are issued to staff to host Tapestry. They are PIN password protected and monitored through the schools filtering and monitoring system.
- The schools filtering and monitoring system will identify if inappropriate contact has been made

- All staff are issued with a password protected, work based email. This is to be used at all times related to work based matters.
- Staff receive update training when relevant related to Online Safety.
- Mobile telephones are kept in staff areas and are not to be taken into the classrooms by staff in ratio as per the Safeguarding Policy, there may be occasions at the discretion of the Headteacher, whereby for H&S premises evidence an image must be taken by the Business Manager or other using their mobile phone.
- Staff are permitted to wear smart watches as long as these are used for time-telling purposes only and mobile devices linked to them are not transferring a signal/messages during teaching time when staff are in classrooms.

INTERNET AND ACCETABLE USE

- The Internet is a useful and necessary tool for staff and there are filtering and monitoring systems in place. These are closely monitored so they do not prevent staff from doing their job.
- Daily reports are provided to the DSL at each school in relation to staff access of pages that have been blocked or sites access that are deemed to be inappropriate and ensure that staff conduct is appropriate. The DSL is responsible for the monitoring of these and will discuss inappropriate or blocked sites with individuals. Records of this will be kept by the DSL.
- If staff come across sites or pages that they deem to be inappropriate or unsuitable on-line materials, the website must be reported to the DSL immediately.
- Any discovery or complaint of staff misuse, will be investigated by the DSL and other policies (such as disciplinary) will be applied where necessary.
- Children will not be allowed access on the Internet.
- The IT information systems, internet and email may not be used for private purposes
- No member of staff should install any software or hardware 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 Executive Headteacher, Head of School or Family Centre Manager immediately.
- Information is shared with parents via Newsletters and Social Media about how to keep their children safe online.
- Children are taught about keeping themselves safe in a variety of ways through our PSED curriculum.

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

The Safeguarding Policy, Staff Behaviour Policy and Staff Handbook give further information to employees regarding the safe use of IT, internet and Online safety and should be read in conjunction with this policy.

Approved by the Governing Body: March 2024
To be reviewed by: March 2025
Relevant for:-

Nursery: Yes	**Parents**: Yes