PARK SCHOOL AND NURSERY - STAFF ICT ACCEPTABLE USE POLICY

To be read with: e-Safety Policy, Privacy Notice

1. AGREEMENT

1.1 As a professional organisation with responsibility for children’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 school’s 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 this Acceptable Use Policy.

2. THIS IS NOT AN EXHAUSTIVE LIST AND ALL MEMBERS OF STAFF ARE REMINDED THAT ICT USE SHOULD BE CONSISTENT WITH THE SCHOOL ETHOS, OTHER APPROPRIATE POLICIES AND THE LAW.

2.1 I understand that Information Systems and ICT include networks, data and data storage, online and offline communication technologies and access devices. Examples include mobile phones, PDAs, digital cameras, email and social media sites.

2.2 School owned information systems must be used appropriately. I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.

2.3 I understand that any hardware and software provided by my workplace for staff use can only be used by members of staff and only for educational or admin use. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or locking my login as appropriate.

2.4 I will respect system security and I will not disclose any password or security information. I will use a ‘strong’ password (a strong password has numbers, letters and symbols, with 8 or more characters, does not contain a dictionary word and is only used on one system).

2.5 I will not attempt to install any purchased or downloaded software, including browser toolbars, or hardware without permission from the ICT consultant.

2.6 I will ensure that any personal data of pupils, staff or parents/carers is kept in accordance with the Data Protection Act 2018. This means that all personal data will be obtained and processed fairly and lawfully, only kept for specific purposes, held no longer than necessary and will be kept private and secure with appropriate security measures in place, whether used in the workplace, hosted online (only within countries or sites with suitable data protection controls) or accessed remotely. Any data which is being removed from the school site (such as via email or on memory sticks or CDs) will be encrypted by a method approved by the school. Any images or videos of pupils will only be used as stated in the letter “Using Images of Children”, which has been provided to all parents.

2.7 I will not keep professional documents which contain school-related sensitive or personal information (including images, files, videos etc.) on any personal devices (such as laptops, digital cameras, mobile phones), unless they are secured and encrypted. I will protect the devices in my care from unapproved access or theft.

2.8 I will not store any personal information on the school computer system that is unrelated to school activities, such as personal photographs, files or financial information.

2.9 I will respect copyright and intellectual property rights.

2.10 I have read and understood the school e-Safety policy which covers the requirements for safe ICT use, including using appropriate devices, safe use of social media websites and the supervision of pupils within the classroom and other working spaces.

2.11 I will report all incidents of concern regarding children's online safety to the School Designated Senior Person for Safeguarding and/or the e-Safety Coordinator as soon as possible. I will report any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable websites to the e-Safety Coordinator as soon as possible using the form held in the ICT suite. The form is to be given to the e-safety coordinator who will act accordingly.

2.12 I will comply with the guidelines regarding Personal Electronic Devices (including personal mobile phones) within this Acceptable Use Policy.

2.13 I will not attempt to bypass any filtering and/or security systems put in place by the school. If I suspect a computer or system has been damaged or affected by a virus or other malware or if I have lost any school related documents or files, then I will report this to ICT Support as soon as possible. (Report by using the appropriate icon on the computer).

2.14 I will respect, when using email, the guidelines within this Acceptable Use Policy.

2.15 My electronic communications with pupils, parents/carers and other professionals will only take place via work approved communication channels e.g. via a school provided email address or telephone number. Any pre-existing relationships which may compromise this should be discussed with the Headteacher.

2.16 My use of ICT and information systems will always be compatible with my professional role, whether using school or personal systems. This includes the use of email, text, social media, social networking, gaming, web publications and any other devices or websites. My use of ICT will not interfere with my work duties and will be in accordance with current UK Law.

2.17 I am aware that my online conduct out of school could have an impact on my role and reputation within school. Civil, legal or disciplinary action could be taken if I am found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in my professional abilities.

2.18 I will not create, transmit, display, publish or forward any material that is likely to harass, cause offence, inconvenience or needless anxiety to any other person.

2.19 I will promote e-Safety with the pupils in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create.

2.20 If I have any queries or questions regarding safe and professional practice online either in school or off site, then I will raise them with the e-Safety Coordinator or the Headteacher.

2.21 I understand that my use of the information systems, Internet and email may be monitored and recorded to ensure policy compliance. Internet and network use may be traced back to the individual user.

2.22 Where the School believes unauthorised and/or inappropriate use of the service's information system or unacceptable or inappropriate behaviour may be taking place, it will invoke its disciplinary procedure. If the School suspects that the system may be being used for criminal purposes or for storing unlawful text, imagery or sound, the matter will be brought to the attention of the relevant law enforcement organisation.

3. GUIDELINES RE THE USE BY STAFF OF PERSONAL MOBILE PHONES, TABLETS, CAMERAS ("Personal Electronic Devices").

3.1 Aims

- Protect the school against risk of problematical incidents
- Protect staff against false allegations or difficult situations

- Comply with EYFS requirements (the EYFS now requires that safeguarding policies and procedures must cover the use of mobile phones and cameras in the setting to minimise the risk of inappropriate sharing of images.
- In relation to the whole school, to comply with best practice as advised by ISI
- Maintain a professional image in the eyes of pupils, parents and visitors

3.2 Guidance

3.2.1 Personal Electronic Devices must be switched off in school, except for in the staff room or in staff meetings, or otherwise with the permission of the Headteacher. Personal Electronic Devices using the school wi-fi need to be registered with the school's ICT department. It is recommended that Personal Electronic Devices are password protected and insured.

3.2.2 Where staff are with pupils off-site, Personal Electronic Devices should not be used, except when staff are off-duty and in a place away from children.

3.2.3 Personal mobile phones may be used at any time if their use is the best way of dealing with an urgent issue of Health and Safety.

3.2.4 Some non-teaching members of staff have been given permission to use personal mobile phones in school (beyond the staff room and staff meetings) for work related administrative and communication purposes. Staff falling into this category include the Headteacher, members of the Bursar's department, the ICT consultant, members of the site-management team, the chef manager and staff in the School Office. Use of personal mobile phones by these members of staff is constantly monitored by the Bursar.

3.2.5 Visitors, including other professionals and contractors, are made aware by the School Office or by the Bursar's department that they are not to use their mobile phone where children are present.

3.2.6 All photos or videos of children taken by staff must be taken and stored on school equipment only.

3.2.7 When giving out a phone contact number for parents (e.g. when there is a meeting place or collection point during a trip/match off site), the number should be a school mobile phone number.

3.2.8 Phone calls to parents should be from a school phone

3.2.9 Staff are advised to provide their work place contact number to their family members, own children's schools/settings for use in the event of an emergency.

3.3 The effectiveness of this policy is formally discussed once a month by discussion in senior staff meeting. Senior staff are constantly monitoring the site for compliance with this policy. All staff are asked to report any infringement of this policy to the Designated Senior Person for Safeguarding

4. GUIDELINES RE STAFF USE OF EMAIL.

4.1 General principles

4.1.1 We work on a small site where we see each other a lot. We also have a terrific team spirit and excellent personal relationships which are hugely important to protect and nurture. There are dangers of using email which can impact negatively upon these strengths.

4.1.2 Staff should be aware that Data Protection legislation may require the school to disclose the contents of pupils' files to parents. Emails about pupils must therefore be regarded as potentially public documents.

4.1.3 We should endeavour to avoid sending emails which criticise individuals. This is especially the case where emails are sent to more than one person

4.1.4 "Think before you click!". If we really do have to send an email on a difficult issue, then whenever there is time to do so, we stick it into the draft box and reread it later (preferably after having slept on it!). It is also useful to show such drafts to a trusted friend or colleague before sending it (as long as it is not betraying confidentiality).

4.1.5 We check our email at least once every 24 hours on working days.

4.1.6 When sending emails to colleagues outside of our normal working hours we cannot assume that this email will be read before the next working day.

4.1.7 In the case of urgent messages, other means of communication than email should be used so that we know the message has been received.

4.1.8 When opening attachments on received e-mails, this should be done bearing in mind e-mail security.

4.2 Emails to and from parents

4.2.1 Communicating with parents is very important to us as a school and lines of communication need to be open. However, as a general policy we try to avoid a situation where parents email us direct to our personal Park School email addresses. This often requires care in ensuring that an email address does not appear in the text of an email or in the recipient boxes etc.

4.2.2 If parents really do need to send an email to a member of teaching staff, it should be sent to parkschool-year?@parkschool.co.uk, so the member of staff can access it through the year group inbox or office@parkschool.co.uk, asking for the message to be relayed to the member of staff. Where an email is received from a parent it is important to get back to the parent (even if it is just a holding reply) within 24 hours or receiving it, and if possible by the end of the day on which it has been received. We can reply either by picking up the phone, by catching the parents in school, by writing in the homework diary, or by sending an email from the year group email address.

4.2.3 Should a parent email a member of teaching staff direct, then the member of staff may say politely that it is the general policy of the school to avoid the direct emailing of staff by parents. . Reply to the email from the year group email address and advise them to use this line of communication in future.

4.3 Emails to and from pupils

4.3.1 Emails between staff and pupils are sent via the Microsoft Office 365 system.

4.3.2 Staff should not send emails to individual pupils.

4.3.3 Pupils have been told that they must not email staff using individual email addresses.