

This school is committed to safeguarding and promoting the welfare of children and young people and expects all staff and volunteers to share this commitment.



PARKSIDE
SCHOOL

Edition: 2 April 2020

INFORMATION TECHNOLOGY ACCEPTABLE USE POLICY

**This policy is applicable to the whole School,
including the Early Years Foundation Stage (EYFS)**

References:

ISI: Commentary on the Regulatory Requirements 2019-09 (September 2019)
Keeping Children Safe in Education (September 2019) (*KCSIE*)
Data Protection Act 2018 (May 2018) (*DPA*)
General Data Protection Regulation (May 2018) (*GDPR*)
Prevent Duty Guidance: for England and Wales (July 2015) (*Prevent*)
The use of social media for online radicalisation (July 2015)
Section 26 of the Counter-Terrorism and Security Act 2015
DfE: Preventing and Tackling Bullying (October 2014)
DfE: Cyberbullying: Advice for headteachers and school staff (2014)

1. Introduction

Parkside School (the School) is committed to providing the best possible care and education to its pupils and to safeguarding and promoting the welfare of children and young people.

2. Scope of Policy

This policy applies to all members of the School community, including staff, pupils, parents, and visitors. It is not intended as a comprehensive E-safety Policy. It is intended to be used in conjunction with the school's E-safety Policy, which describes a more detailed framework for safe use of IT systems in schools (including monitoring).

3. Aims

New technologies have become integral to our lives in today's society, both within and outside School. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone.

- These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning.
- They also bring opportunities for staff to be more creative and productive in their work.
- The School will try to ensure that staff and pupils have good access to IT to enhance their work and opportunities for pupils' learning and will, in return expect staff and pupils to agree to be responsible users.
- It is important that appropriate limitations are placed on the use of the School's IT facilities in order to protect users and the School's IT systems from accidental or deliberate misuse that could put the security of the systems and users at risk.
- In order to protect staff, pupils and the School, it is also important that staff and pupils adhere to the School's guidelines for the use of electronic devices such as cameras and mobile phones and, where appropriate, for the use of social media websites such as Facebook or Twitter.
- Staff are asked to sign to confirm that they have read and understood the IT Acceptable Use and E-safety Policies; a copy of the Agreement will be held in staff files. See Appendix 1.
- Pupils have their own Agreement which must be signed annually by both pupils and their parents. See Appendix 2.
- The School also has a Bring your own device Policy (BYOD) with Terms and conditions which must be signed for. See Appendix 3.

Links to other policies

- Anti-Bullying Policy
- Anti-Cyber Bullying Policy
- BYOD Policy
- Data Protection policies
- Disaster Recovery Plan
- E-safety Policy
- Privacy Notices
- Remote Access Policy
- Remote Learning Policy
- Safeguarding Policy
- Staff Code of Conduct
- Staff Social Media Policy
- Storage & Retention of Records Policy
- Use of Images Policy
- Whistleblowing Policy

4. Online behaviour

As a member of the School community you should follow these principles in all of your online activities:

- Ensure that your online communications, and any content you share online, are respectful of others and composed in a way you would wish to stand by.
- Do not access, create or share content that is illegal, deceptive, or likely to offend other members of the School community (for example, content that is obscene, promotes violence, discrimination, extremism or raises safeguarding issues).
- Respect the privacy of others. Do not share photos, videos, contact details, or other information about members of the School community, even if the content is not shared publicly without going through official channels and obtaining permission.
- Do not access or share material that infringes copyright, and do not claim the work of others as your own.
- Do not use the internet to distribute malicious software, to damage, interfere with, or gain unauthorised access to the computer systems of others, or carry out illegal activities.
- Staff should not use their personal email, or social media accounts to contact pupils or parents, and vice versa with pupils and parents.

5. Using the School's IT systems

Whenever you use the School's IT systems (including by connecting your own device to the network) you should follow these principles:

- Only access School IT systems using your own username and password. Do not share your username or password with anyone else.
- Do not attempt to circumvent the content filters or other security measures installed on the School's IT systems, and do not attempt to access parts of the system that you do not have permission to access.
- Do not attempt to install software on, or otherwise alter, School IT systems.
- Do not use the School's IT systems in a way that breaches the principles of online behaviour set out above.
- Remember that the School monitors use of the School's IT systems, and that the School can view content accessed or sent via its systems.

6. Password security guidelines (See E-safety Policy)

Passwords protect the School's network and computer system and are your responsibility.

- They should not be obvious (for example "password", 123456, a family name or birthdays), and nor should they be the same as your widely-used personal passwords.
- You should not let anyone else know your password, nor keep a list of passwords where they may be accessed, and must change it immediately if it appears to be compromised.
- You should not attempt to gain unauthorised access to anyone else's computer or to confidential information to which you do not have access rights.

7. Use of Property

Any property belonging to the School should be treated with respect and care, and used only in accordance with any training and policies provided. You must report any faults or breakages without delay to the Bursar.

8. Use of School systems

The provision of School email accounts, Wi-Fi and internet access is for official school business, administration and education. Staff and pupils should keep their personal, family and social lives separate from their School IT use and limit as far as possible any personal use of these accounts. Again, please be aware of the School's right to monitor and access web history and email use.

9. Use of personal devices or accounts and working remotely

All official School business must be conducted on School systems, and it is not permissible to use personal email accounts for School business.

- Any use of personal devices for School purposes, and any removal of personal data or confidential information from School systems – by any means including email, printing, file transfer, cloud or (encrypted) memory stick – must be registered and approved by the IT Department.
- Where permission is given for use of personal devices, e.g. when providing Remote Learning - these must be subject to appropriate safeguards in line with all policies of the School. This includes our protocols for Safeguarding, SEND, Health & Safety and Data Protection.

10. Monitoring and access

Staff, parents and pupils should be aware that School email and internet usage (including through School Wi-Fi) will be monitored for safeguarding, conduct and performance purposes, and both web history and School email accounts may be accessed by the School where necessary for a lawful purpose – including serious conduct or welfare concerns, extremism and the protection of others.

11. Retention of digital data

Staff and pupils must be aware that all emails sent or received on School systems will be routinely deleted after 2 years and email accounts will be closed (and the contents deleted) after 1 year of that person leaving the School.

- Important information that is necessary to be kept should be held on the relevant personnel or pupil file, **not** kept in personal folders, archives or inboxes.
- It is the responsibility of each account user to ensure that important information is retained in the right place or, where applicable, provided to the right colleague. That way no important information should ever be lost as a result of the School's email deletion protocol.
- If you consider that reasons exist for the protocol not to apply, or need assistance in how to retain and appropriately archive data, please contact the Compliance Officer.

12. Breach reporting (See Data Breach Management Policy)

- Please refer to the Policy above should data be lost, miss-treated or compromised.
- If in any doubt as to whether there may have been a data breach, please contact the Privacy Officer as soon as possible.

13. Monitoring, Evaluation and Review

This Policy is monitored, evaluated and reviewed on an annual basis by the Senior Leadership Team.

AG

Reviewed: Autumn Term 2019

Approved by the Governors' Education Committee: 29.1.19

Next review: Autumn Term 2020

Appendix 1:

Staff IT Acceptable Use/E-safety Agreement



PARKSIDE
SCHOOL

Please sign and date the following statement to indicate that you have read, understood and agree to abide by the School's IT Policies. A copy will be held on your staff file.

1. I understand that I must use School IT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the IT systems and other users.
2. I understand that the School may monitor my use of the IT systems, email and other digital communications.
3. I understand that the School IT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the School.
4. I will not disclose my username or password to anyone else, nor will I try to use any person's username or password.
5. I will immediately report any illegal, inappropriate or harmful material or incident I become aware of to the appropriate person. I will not create, transmit or cause to be transmitted any such material.
6. I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
7. I will communicate with others in a professional manner; I will not use aggressive or inappropriate language.
8. I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the School's policy on the use of digital images and Data Protection Policies.
9. When using chat and social networking sites either in or outside school time, I will adhere to the School's policy on social networking (See Staff Social Media Policy).
10. I will only communicate with pupils and parents/carers using official School systems. Any such communication will be professional in tone and manner. (See Presentation Policy)
11. I will not engage in any on-line activity that may compromise my professional responsibilities or bring the School into disrepute.
12. I will not open any attachments to emails, unless the source is known and trusted, due to the risk of viruses or other harmful programs.
13. I will not attempt to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
14. I understand that the Data Protection Policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by the School policy to disclose such information to an appropriate authority.
15. I appreciate that electronic mail is relatively insecure and will consider security needs and confidentiality before transmission.
16. I understand that I am responsible for all my actions in and out of School.
17. When working remotely, I understand the same protocols as above apply away from school and understand our Safeguarding protocols apply also.
18. I understand that this Agreement applies not only to my work and use of School IT equipment in School, but also applies to my use of School IT systems and equipment out of School and my use of personal equipment in School or in situations related to my employment by the School.
19. I understand that failure to comply with this Agreement could result in disciplinary action. This could include a warning, a suspension, referral to Governors, dismissal, and in the event of illegal activities the involvement of the Police.

Staff/volunteer name

Signed

Date

Revised March 2020

Appendix 2:

Pupil IT Acceptable Use / E-safety Agreement:



PARKSIDE
SCHOOL

Please will parents and pupil sign and date the following statement to indicate that you have read, understood and agree to abide by the School's IT Policies.

Pupil IT Acceptable Use / E-safety Agreement:

- I will use iPads, computer, internet and email only for school-related tasks.
- I will look after the equipment and treat it with care.
- I will not search for anything inappropriate on the internet.
- I will tell a teacher straight away if I come across something inappropriate on the internet.
- I will report any mean or rude behaviour to a teacher.
- I will not share my personal information online.
- I will not print without permission from a teacher.
- I will not download any music, videos and programmes without permission from a teacher.
- I will not change screensavers, backgrounds or any other settings.
- I will not be mean or rude to or about anyone online.

Pupil Name

Pupil Signature

Parent Name

Parent Signature

Head of IT & Digital Learning

Revised March 2020

Appendix 3:



PARKSIDE
SCHOOL

Bring Your Own Device (BYOD) User Agreement

Please sign and date the following statement to indicate that you have read, understood and agree to abide by the School's IT Policies. Terms and Conditions overleaf.

Bring Your Own Device (BYOD) User Agreement:

- I will only use my IT device (iPad, laptop, tablet) and School memory sticks which have been checked and validated by the Head of IT & Digital Learning.
- I will use my IT device for school-related / educational tasks only.
- I will send my work to the teacher by email or on a School approved memory stick at the end of each lesson / prep.
- I understand I am responsible for ensuring I have cut and stuck in any printed work into my exercise book / folder in place of hand-written work.
- I will not connect to the internet / use WIFI.
- I will not distract others when I use my IT device.
- I will not play games, text others, email others or send photos / videos to anybody.
- I will keep my IT device at the Laptop Hotel for safekeeping when not in use.
- I will check my IT device daily to ensure it is fully charged and has no obvious defects and is free from unsuitable material or viruses.
- I will not bring in a charger as I understand my IT device must be fully charged before arrival.
- I understand that there are consequences if I misuse my IT device.
- I understand that I bring in my personal IT device entirely at my own risk.

Pupil Name

Pupil Signature

Date

Parent Name

Parent Signature

Date

Head of IT & Digital Learning

Revised March 2020

Appendix 3 continued:

Bring Your Own Device (BYOD) Terms & Conditions

Please refer to the BYOD Policy.

- Overview:
 1. Pupils must use School IT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the IT systems and other users.
 2. Pupils are expected to use personal IT devices in accordance with this Policy and by using any such device in School, pupils agree to be bound by the additional School rules and requirements set out in this Policy.
 3. IT Devices in this instance refer to laptops and Tablet devices NOT mobile phones.
 4. Pupils must check their personal IT device daily to ensure the device is charged, free from unsuitable material and free from viruses etc. before bringing the device into School.
 5. Pupils must check their personal IT device daily for basic Health and Safety compliance to ensure it is free from defects. Any personal IT device that has obvious Health and Safety defects should not be brought in.
 6. Under no circumstances are pupils permitted to bring into School or use privately owned chargers for personal devices.

- Consequences for misuse/disruption:

If there is misuse/disruption the personal IT device will be confiscated with an escalation process for continuing issues in place. Ultimately the pupil will lose the privilege of bringing it to School.

- School Liability Statement:

Pupils bring their personal IT devices to use at Parkside School at their own risk. Pupils are expected to act responsibly with regards to their own device, keeping it up to date via regular anti-virus and operating system updates and as secure as possible. It is their duty to be responsible for the upkeep and protection of their devices. Parkside School is in no way responsible for:

 - a. Personal devices that are broken whilst at School or during School-sponsored activities.
 - b. Any data lost on personal devices.
 - c. Personal devices that are lost or stolen at School or during School-sponsored activities.
 - d. Maintenance or upkeep of any device (keeping it charged, installing updates or upgrades, fixing any software or hardware issues).
 - e. Parents should ensure they have adequate insurance cover in place to cover the cost of repair/replacement of a personal IT device in the event of loss/damage to the device.

- BYOD User Agreement:

By using your own personal IT device in School you agree to the User Agreement of this Policy and the associated Frequently Asked Questions. Please note:

 - Currently approved device types are: Laptops and Tablets only (No mobile phones/wearable technology)
 - That by connecting a personal device to the Schools system you confirm you have understood the School's BYOD Policy and you agree to be bound by the rules and regulations contained in the BYOD, Mobile Phone, IT Acceptable Use, and Discipline & Behaviour Management policies.
 - That you understand that the use of a personal IT device in School is a privilege not a right and agree to use the device for learning only.
 - You agree not to connect to any wireless or networking service other than that supplied by Parkside School while using my personal IT device in the School.
 - You understand that pupils are solely responsible for the correct care, safety and security of my personal IT device when in School.

- Disclaimer - please read carefully
Parents. Parkside School accepts no liability in respect of any loss/damage to personal IT devices while at School, during School-sponsored activities or in transit. The decision to bring a personal IT device into School rests with the pupil and their parents, as does the liability for any loss/damage that may result from the use of a personal IT device in School. You should understand that by allowing pupils to bring personal IT devices into School, you agree to this disclaimer.