Parson Street Primary School

Acceptable Use Policy

2023-2024

ETHOS STATEMENT

It is the aim of the Governing Body of Parson Street Primary School to support the implementation of policies and procedures which develop the skills our children need to achieve our vision of:

"Empowering all to create opportunities for life-long learners in our communities."

INTRODUCTION

In order to exploit the many educational and social benefits of new technologies, learners and staff need opportunities to create, collaborate, communicate and explore in the digital world, using multiple devices from multiple locations. School staff are also now actively encouraged to use platforms such as Twitter for CPD opportunities. However, at times, the use of IT for these purposes may encounter risks.

It is now recognised that e-safety risks are posed more by behaviours and values online than the technology itself. Therefore, the approach must be one of empowering learners and staff to develop safe and responsible behaviours to safeguard themselves and others rather than restricting access to the use of various technologies. We attempt to continually keep up-to-date with the latest e-safety risks posed both in and out of school.

AIMS

The purpose of this policy is to:

- Establish the ground rules we have in school for using various technologies;
- Offer guidelines which will safeguard and protect learners and staff from misuse of technology;
- Raise awareness of e-safety amongst learners and staff;
- Ensure all staff comply with the new GDPR.

The school believes that the benefits to learners and staff from access to the range of technology available far exceed the disadvantages. Ultimately, the responsibility for setting and conveying the standards that we expect in relation to use of technologies is one we share with parents and guardians.

The guidance and regulations outlined in this policy will, if adhered to, help to ensure that our infrastructure is a robust and secure one which will offer numerous benefits to all users.

USE OF TECHNOLOGY

All users (learners and staff) are encouraged to make use of the school's Computing facilities for educational purposes. Technology such as mobile phones, tablets, MP3 players, Personal Digital Assistants (PDA), memory cards, **encrypted USB storage devices**, digital or video cameras should be used responsibly and in accordance with the principles outlined in this policy, even if not connected to the school network. All users must take responsibility for their own use of new technologies, making sure that they use technology safely, responsibly and legally. They must be active

participants in e-safety education, taking personal responsibility for their awareness of the opportunities and risks posed by new technologies.

NETWORK SECURITY

All staff and pupil users of the school network are issued with login access to the school network. Protection of login accounts is the responsibility of the individual and passwords should not be shared **in any circumstances.** All users have a duty to protect their passwords and personal network logins and should log off or lock their network account when leaving workstations unattended. Any attempts to access, corrupt or destroy other users' data or compromise the privacy of others in any way, using any technology, is unacceptable.

The security of our network and associated web-based programmes, (e.g. SIMs, Arbor, Sharepoint, Office 365) is of paramount importance due to the data that it has stored. Users are reminded that Parson Street Primary School reserves the right to monitor the curriculum and admin network activity and communication is monitored by the appropriate persons. This includes monitoring of any personal and private communications made via the school network. Any misuse of the network and its facilities may result in the user having their account suspended and possible disciplinary action.

The servers have systems in place to back up data and prevent the introduction of a virus to the network. As a result, access to these is limited to the IT Team. Permission must be sought from the IT Team for anyone else wishing to access the servers. Learners MUST NOT access the server at any time.

Finally, all users have a duty to respect the technical safeguards which are in place and should not attempt to introduce a virus or malicious code or bypass any network security systems. Any attempt to breach technical safeguards, conceal network identities or gain unauthorised access to the systems and services is unacceptable. It is the duty of all users to report any suspected or known failings in technical safeguards which may become apparent when using the systems and services.

To protect the safety and security of our network, users are reminded that they must not download or install any software/hardware or attempt to use any form of hacking systems to gain access to an unauthorised area.

ACCESSING THE INTERNET

The internet is used commonly throughout all aspects of the curriculum both by learners and by staff. Whilst every effort is made to safeguard learners in this environment, children are spoken to regularly about e-safety so that they can browse this medium safely and sensibly making decisions about the appropriateness of the material they come across.

Parson Street Primary School will use a filtered internet service, which will minimise the chances of pupils encountering undesirable material. The filtering service is managed by Bristol City Council. The filtering system is also supported by the management of an 'in-house' monitoring system.

Parson Street Primary School will only allow children to use the internet when there is a responsible adult present to supervise. However, it is unrealistic to suppose that the teacher's attention will always be directed toward the computer screen. Learners are therefore reminded of responsible internet use and are asked to sign the acceptable use agreement (see appendix 1).

Children are taught what to do if something appears on the screen that they are unsure about or do not like. The children will be asked to turn the monitor screen off and tell an adult straight away.

The use of public chat rooms and /or messaging services is not allowed unless prior permission has been obtained from the head teacher which may be granted in cases where it may be used to support educational activity. In this case school users must not use their personal account and should, instead, create a school-based account.

USE OF EMAIL/SOCIAL NETWORKING

All members of staff have access to an individual email account and are required to check them daily. There is the opportunity for classes to have email accounts and staff can arrange this in consultation with the IT Team. Email is recognised as an effective and powerful form of communication and awareness is therefore raised of general email netiquette (see appendix 2). Parents wishing to correspond via email should be directed to the enquiry email address: office@parsonstreet.com. If staff communicate with parents/carers via email they must maintain the professionalism that would be evident if they were speaking with the parent/carer in person. Any issues should immediately be reported to the Head Teacher/Deputy Head Teacher.

Each class has its own Class Dojo account which parents are encouraged to sign up to. The messaging facility on this platform should be used in the same way as an email communication and therefore must maintain the same professionalism as outlined in the previous paragraph.

The use of social networking sites, e.g. Facebook, is strictly forbidden on the school network unless specific permission has been given. The school has a Twitter account so allows and encourages use of this on the school network. However, children's knowledge about the correct usage of these platforms is raised through regular e-safety lessons. Staff choosing to access social networking sites should not use this as a form of communication with any pupil. This is imperative in the interests of safeguarding for both staff and pupil.

Use of such networking sites should not bring the individual or the school into disrepute. All users have a responsibility to report any known misuse of technology including the unacceptable behaviour of others.

If a user receives an offensive or upsetting email then this should be stored and shared with the IT Team, Head Teacher or Assistant Head teachers immediately.

USE OF OTHER TECHNOLOGIES

WI-FI ACCESS
Wi-Fi access is available throughout the school and school owned devices can be securely connected to our network using this facility. Personal devices may be connected to the network with prior permission but must strictly adhere to the same rules.

MOBILE PHONES/COMMUNICATION DEVICES
Staff must NEVER communicate with learners via the use of mobile phones. Any staff found sharing their personal phone numbers with learners may face disciplinary action.

No communications device, whether school provided or personally owned, may be used for the bullying or harassment of others in any form. This applies to staff and pupil use. All users should be aware that in certain circumstances where unacceptable use is suspected, enhanced monitoring and procedures may come into action, including the power to check and/or confiscate personal technologies such as mobile phones. Staff should not use personal mobile phones to take photographs of pupils unless specific permission has been granted by the Headteacher. If permission is granted then the photographs should be deleted from the phone immediately after being downloaded to the school network.

CAMERAS
At Parson Street we encourage the use of digital imagery by both pupils and staff as it has many uses including use for assessment evidence, display around the school, sharing with parents/press etc. and displaying on the website/Twitter. However, pictures of pupils will only be used in external circumstances (e.g. website or press) with the prior permission of parents or guardians (see office for current list of permissions for photographs). All lists granting permission will be in accordance to GDPR. Staff must only use school owned devices when taking pictures of children unless specific permission has been granted otherwise.

PRINTING/PHOTOCOPYING
Staff are provided with colour and black and white printing/copying facilities. All users are encouraged to consider the need to print colour documents and to avoid any wastage by carefully selecting the printer they intend to print to. User printing/copying levels can be logged and monitored.

Staff should not share their user access codes with other members of staff for the photocopier and must remember to log out when they have finished using this facility. Exceptions can be made if a member of staff is asked to collect printing/copy for another member of staff. However, use of the details without the staff member's permission is forbidden.

LAPTOPS / iPADS
A number of staff are provided with a school laptop, iPad or other device for them to use throughout the duration of their employment at Parson Street Primary School. These may be connected to the school network via individual user accounts and may also be taken off site for staff to complete schoolwork at home.

Staff use of the device is bound by the terms and conditions outlined in the 'IT Loan Agreement' which is signed upon receipt of the device(s). Individual staff are responsible for the device assigned to them and may not exchange this with another member of staff.

Staff adherence to the acceptable use agreement (appendix 1) must also be obtained annually to remind staff of their responsibilities when using technologies for their professional role. Devices assigned to staff may also be used for personal reasons except where this violates the terms and conditions of use or of the AUP.

Software must not be uninstalled or removed from the individual laptop in the same way that it must not be installed without the prior permission of the head teacher, IT Team or the Key Area Leader. If staff require APPs to be downloaded onto school iPads, they should gain permission from IT Support who will authorise and then pass on to the IT Team to install.

If an IT issue arises, it must be logged with the helpdesk: helpdesk@tilaacademies.co.uk. If a staff member feels an issue has not been dealt with, they can email head of IT helpdesk directly on shardwell@bridgelearningcampus.com

DOCUMENT STORAGE:
All users of the network have an individual folder/drive where they can store their personal documents. This drive is only accessible by the individual user and the administrator of the network. There are also 'shared' drives where documents can be shared with colleagues and/or learners.

Staff are permitted to use encrypted USB storage devices in order to back up any of their data but must be aware of the guidelines about the storage of pupil data and the need to keep this secure. The use of any unencrypted USB storage devices is strictly prohibited; other methods of accessing school data via an encrypted connection at home have been provided by Parson Street Primary School (Home Access Plus+).

MAINTENANCE OF TECHNOLOGY FACILITIES

Technical support is provided by TILA IT Team to ensure that the computing facilities at this school effectively support teaching and learning. All users have a duty to raise a ticket via email to report any faults immediately (helpdesk@tilacademies.co.uk).

All users should use network technologies responsibly. Wasting staff effort or networked resources, or using resources in such a way so as to diminish the service for other network users, is unacceptable.

Users should not attempt to repair any equipment themselves and should not attempt to use any equipment which may be dangerous to do so. The Key Area Leader and/or the IT Team can be contacted if you have any questions about the use of any new technologies.

DISCIPLINARY PROCEDURES

Those who misuse technologies or who break the acceptable use agreements may be subject to disciplinary procedures.

KEY RESPONSIBILITIES

FOR LEARNERS

- Read and agree to the rules outlined in the Acceptable Use Agreement.
- Take responsibility for keeping themselves and others safe.
- Take responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.

- Behave sensibly when using any technology in order to limit any risks.
- Respect the feelings, rights and values of others.
- Seek help from a trusted adult if things go wrong, and support others who may be experiencing e-safety/cyberbullying issues.
- Discuss e-safety with parents in an open and honest way.

FOR STAFF

- Contribute to the development of e-safety policies.
- Read and agree to the rules outlined in the Acceptable Use Agreement.
- Take responsibility for the security of systems and data.
- Have an awareness of e-safety issues and how they relate to the pupils in their care.
- Model good practice in using new and emerging technologies, emphasising positive learning opportunities rather than focussing on negatives.
- Embed e-safety education in curriculum delivery wherever possible.
- Know how and when to escalate e-safety issues.
- Maintain a professional conduct in their personal use of technology, both within and outside school.
- Take personal responsibility for their professional development in this area.
- Comply with the requirements of the new GDPR.

FOR THE SENIOR LEADERSHIP TEAM

- Develop and promote an ethos where e-safety is clearly valued.
- Support the Key Area Leader the development of an e-safety culture.
- Make appropriate resources available to support the development of an e-safe culture.
- Support/handle appropriately incidents of misuse of technologies.
- Take ultimate responsibility for e-safety incidents.
- Monitor compliance with the new GDPR across the school.

FOR THE KEY AREA LEADER

- Develop an e-safe culture and act as a name point of contact for all e-safety issues (under the direction of the SLT).
- Promote e-safety to all users and support them in their understanding of the issues.
- Ensure that e-safety is embedded into CPD for staff and curriculum coverage for learners.
- Ensure that e-safety is promoted to parents and guardians.
- Maintain an e-safety incident log and report these to the SLT on a regular basis.
- Develop an understanding of the relevant legislation, liaise with the LA or other appropriate bodies and review/update e-safety procedures on a regular basis.

FOR THE IT TEAM

- Support the Key Area Leader in the implementation of e-safety procedures and practises.
- Provide support to the technical infrastructure to support e-safe practices while still maximising learning opportunities.
- Take responsibility for ensuring back-up systems are working and that data is stored securely on the school network.
- Develop an understanding of e-safety legislation as it relates to the technical infrastructure and advise the Key Area Leader of actions as appropriate.

STAFF CONSULTATION

All staff are governed by the terms of the 'Acceptable Use Agreement'.

All staff including teachers, supply staff, learning support assistants and support staff, will be provided with a copy of this policy.

Staff should be aware that network usage can be monitored and traced to the individual user. Discretion and professional conduct is essential.

The monitoring of network usage is a sensitive matter. Staff who operate monitoring procedures should work in consultation with the Senior Leadership Team, particularly where a misuse of the School's Network has been identified.

COMPLAINTS

- Responsibility for handling incidents will be delegated to a senior member of staff.
- Any complaint about staff misuse must be referred to the Head Teacher/Deputy Head Teacher.
- Pupils and parents will be informed of the complaints procedure.
- Parents and pupils will need to work in partnership with staff to resolve issues.
- There may be occasions when the police must be contacted.
- Early contact could be made to establish the legal position and discuss strategies.
- Sanctions available include:
  - interview/counselling by senior member of staff;
  - informing parents or carers;
  - removal of internet or computer access for a period of time.

Appendix Pupil Acceptable Use Agreement

School policy

Digital technologies have become integral to the lives of children, both within schools and outside school. These 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. Children should have an entitlement to safe access to these digital technologies.

This acceptable use agreement is intended to ensure:

- That children will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and will have good access to digital technologies to enhance their learning and will, in return, expect the *pupils* to agree to be responsible users.

I agree that I will:

- I will ask a teacher or suitable adult if I want to use the computers/tablets
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have made a mistake
- I know that if I break the rules I might not be allowed to use a computer/tablet
- Always keep my passwords a secret
- Only visit websites which are appropriate and useful to my learning
- Tell my teacher or an adult I trust if anything from the internet makes me feel scared or upset, or if I feel it is inappropriate
- Make sure any messages I send are polite and respectful. Not send or reply to any 'unkind' messages using email, MSN, Facebook, Snapchat or other similar sites (whether in or out of school)
- Not bring my mobile phone to school if I have one (unless previously agreed with the headteacher). Store my mobile phone in the Office as required during the school day and only give my telephone number to people I know and trust
- Only use the login account I have been provided with at school and make sure I log out when I have finished
- Always keep my personal details private and not share them with other people on the internet
- Not put photographs of myself or others on the internet without checking with an adult first
- I will not arrange to meet anyone I 'meet' on the internet without discussing it with an adult I trust
- Not install my own software onto school computers
- Respect and look after school computing equipment and report any faults to my class teacher

NAME:	**DATE:**

PARENTAL ACKNOWEDLEGEMENT - I have read through the Acceptable Use Agreement for pupils and know the rules that my child is asked to adhere to. I will support the school in enforcing these rules so that my child access technology in an online-safe manner. Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school's work

SIGNED:	**DATE:**

Permission Form

Parent/Carers Name:
Student/Pupil Name:
As the parent/carer of the above student give permission for my child to have access to the internet and to ICT systems at school.
I know that my child has signed an acceptable use agreement and has received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.
I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.
I understand that my child's activity on the systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the acceptable use agreement.
I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's online safety.

This form will be stored electronically.
Staff will have access to the permissions given
The information from this form will be stored on the school information platform for the length of your child's time at Parson Street Primary School

Signed:

Staff (and Volunteer) Acceptable Use Policy Agreement

To ensure that staff are fully aware of their responsibilities with respect to Computing use, they are asked to sign this Acceptable Use Agreement.

I will be professional in my communications and actions when using School systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions. I will ensure that my electronic communications with pupils are compatible with my professional role and cannot be misinterpreted.
- 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 policy on the use of digital/video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use social networking sites in school in accordance with the school's policies.
- I will only communicate with students and parents/carers using official school systems. Any such communication will be professional in tone and manner
- I will not engage in any on-line activity that may compromise my professional responsibilities.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email etc.) out of school, and to the transfer of personal data (digital or paper based) out of school. I will take all reasonable precautions to secure data or equipment taken off the school premises and report any compromises immediately to the Headteacher.

The School and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the campus:

- When I use my mobile devices in school, I will follow the rules set out in this agreement and Mobile Phone Policy, in the same way as if I was using School equipment. I will also follow any additional rules set by the School about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, terrorist or extremist material, adult pornography covered by the Obscene Publications Act) 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.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in School policies or I have been given permission from ITHelpdesk or the Headteacher..
- I will not disable or cause any damage to School equipment, or the equipment belonging to others.

- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School/Academy/LA Personal Data Policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based documents containing personal data must be held in lockable storage.
- I understand that data protection policy requires that any staff or student 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 School policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of Parson Street Primary School:

- I understand that this acceptable use policy applies not only to my work and use of School digital technology equipment in school, but also applies to my use of School systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the campus
- I understand that if I fail to comply with this acceptable use agreement, I could be subject to disciplinary action. This could a warning, disciplinary action and in the event of illegal activities the involvement of the police.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it. I will lock my account or log off whenever I am leaving a computer unattended.
- Disposal of software/hardware used by the school shall only be carried out through the agreed arrangements for the school and I recognise that this will need to be signed off by the Business Manager/Governors. Any equipment disposed of in any other way may be deemed as theft.
- I understand that the network is the property of the school and agree that my use must be compatible with my professional role. I will respect computing systems security and understand that it is a criminal offence to use a computer for a purpose not permitted by its owner.
- I shall carefully consider whether it's necessary to print a document so that my printing does not become excessive or lead to unnecessary waste of resources.
- I shall report any faults/damage of computing equipment to the IT Helpdesk and I understand that jobs will then be prioritised. I shall not attempt to fix faults myself.
- I understand and agree that school will monitor the network and internet use to ensure policy compliance.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

SIGNED:	
PRINT NAME:	
DATE:	

Appendix 2

EMAIL NETIQUETTE

Netiquette refers to the generally accepted rules of behaviour for using the internet. Netiquette rules mainly apply to email and are intended to make the internet a civil place to communicate and share ideas.

- Be clear and concise
- Be pleasant and polite
- Include the topic for your message in the subject area
- Never create or forward a 'chain letter' email
- Verify the recipients before sending an email
- To avoid long distribution lists or to hide private addresses use the BCC (blind carbon copy) section of an email
- Avoid using all capital letters in a message as this could be perceived as threatening
- Don't say something in an email that you wouldn't say or be prepared to discuss in person
- Remember to check your email regularly and discard any unwanted messages from your inbox
- Reply promptly to emails (even if you just acknowledge the receipt of an email)
- Consider what you write in emails as all records of communication are bound by the Freedom of Information Act and are available in the public domain once published.
- Consider use of RN (reply needed) in the subject of the email.

Appendix 3

OTHER SOURCES OF SUPPORT OR INFORMATION RELATED TO E-SAFETY

Child Exploitation and Online Protection Centre:
www.ceop.gov.uk
CEOP is a police organisation focussed on the protection of children and young people from sexual a busy and exploitation – primarily where the use of technology is a factor.

Childnet Internation – Know IT All:
www.childnet.com/kia
Childnet International is a charity that is helping to make the internet a great and safe place for children.

Internet Watch Foundation:
www.iwf.org.uk
The IWF is the UK internet hotline for reporting illegal online content.

ChildLine:
www.childline.org.uk
ChildLine is a service provided by the NSPCC offering a free counselling helpline for children in danger or distress.

National Education Network:
www.nen.gov.uk
The NEN is the UK collaborative network for education, providing schools with a safe, secure and reliable learning environment and direct access to a growing range of online services and content including a range of e-safety resources.

Teachtoday:
www.teachtoday.eu
Teachtoday provides resources for teachers on the responsible and safe use of the new and existing communications technologies.