Parklee Community Primary School

Wardour Street, Atherton, Manchester M46 0AR

E Safety Policy

Our E Safety policy has been written by the school, building on government guidance. It has been agreed by senior management, governors and all staff.

Parklee Community Primary School is currently completing the 360 degree safe self-review tool with the hope of achieving the E Safety Mark Accreditation (Summer Term 2017).

Please read in line with Remote Learning Policy

Date Written: January 2021
Reviewed: January 2022
Reviewed: January 2023
Reviewed: January 2024
Review Date: January 2025

At Parklee we believe that primary education should be a time of opportunity, a happy and meaningful experience that promotes a love of learning, enriches lives and develops life-long skills.

Policy Decisions

The school will maintain a current record of all staff and pupils who are granted access to the school's electronic communications.

All staff will read and sign the School Acceptable Use Policy for pupil access and discuss it with their class, where appropriate.

Parents will be asked to read and sign the School Acceptable Use Policy for pupil access and discuss it with their child, where appropriate. All children will receive a new School Acceptable Use Policy at the start of every academic year (September). These will be included in the children's journals.

All visitors to the school site who require access to the school's network or internet access will be asked to read and sign an Acceptable Use Policy and a guest username and password will be issued (certain internet restrictions will be in place).

When considering access for the vulnerable members of the school community (such as children with special educational needs) the school will make decisions based on the specific needs and understanding(s) of the pupils.

Access to wi-fi and the schools network is password protected. Only users with permission from the Senior Leadership Team will be allowed access.

Internet access for different users will be restricted in accordance with school policy.

Risks

The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of the Internet content, it is not possible to guarantee that access is unsuitable material will never occur via a school computer. Neither the school nor Wigan Council accept liability for the material accessed, or any consequences resulting from Internet use.

The school will use E Safety monitoring software and audit ICT use by staff and pupils on a regular basis to establish if the E Safety policy is adequate and that the implementation of the E Safety policy is appropriate.

Methods to identify, assess and minimise risks will be reviewed regularly.

The security of staff and pupils must be maintained in respect of the school website. Personal details of staff and pupils should not be published unless permission is obtained.

Incidents of Concern

All members of the school community will be informed about the procedure for reporting E Safety concerns (such as breaches of filtering, cyber bullying, illegal content etc).

The E Safety Lead or a member of SLT will record all reported incidents and actions taken in the school E Safety incident log book and in any other relevant areas.

The designated Child Protection Lead and other appropriate members of staff will be informed of any E Safety incidents involving child protection concerns, which will then be escalated appropriately.

The school will manage E Safety incidents in accordance with the school behaviour policy were appropriate.

The school will inform parents/carers of any incidents or concerns as and when required.

After any investigations are completed, the school will debrief, identify lessons learnt, implements any changes required and notify the governing body.

Where there is cause for concern or fear that illegal activity which concerns an adult has taken place or is taking place then the school will contact the Local Authority so that the incident may be escalated to the Police.

Where there is cause for concern that a child is at risk of significant harm the school will contact the Local Authority.

E Safety Complaints

Complaints about Internet misuse will be dealt with under the school's complaints procedure.

Any complaint about staff misuse will be referred to the Headteacher. All E Safety complaints and incidents will be recorded by the school, including actions taken.

Pupils and parents will be informed of the complaints procedure.

Parents and pupils will need to working in partnership with the school to resolve issues.

All members of the school community will need to be aware of the importance of confidentiality and the need to follow the official school procedures for reporting concerns.

Discussions will be held with the local Police Safer Schools and/or Children's

Safeguarding Team to establish procedures for handling potentially illegal issues.
Any issues (including sanctions) will be dealt with according to the school's disciplinary, behaviour and child protection procedures.

All members of the school community will be reminded about safe and appropriate behaviour online and the importance of not posting any content,

comment, images or videos online which cause harm, distress or offence to any other member of the school community.

Internet across the Community

The school will be sensitive to internet related issues experienced by pupils out of school e.g. social networking sites, and or other appropriate advice.

The school will provide appropriate levels of supervision for students who use the internet and technology whilst on the school site.

The school will provide an Acceptable Use Policy for any guest who needs to access the school computer system or internet on site.

Before accessing the school's network all users will need to acknowledge that they have seen and will follow the online E Safety Ambassador Group rules whilst using the computers.

Cyber Bullying / Hate Crime

Cyberbullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Full details are set out in the school's policy on anti-bullying and behaviour.

There are clear procedures in place to support anyone in the school community affected by cyberbullying.

All incidents of cyberbullying reported to school will be recorded.

There will be clear procedures in place to investigate incidents or allegations of cyberbullying.

Pupils, staff and parents/carers will be advised to keep a record of the bullying as evidence.

The school will take steps to identify the bully, where possible and appropriate. This may include examining school system logs, identifying and interviewing possible witnesses, contacting the service provider and the police if necessary.

Pupils, staff and parents/carers will be required to work with the school to support the approach to cyberbullying and the school's E Safety ethos.

Sanctions for those involved in Cyberbullying may include:
The cyberbully will be asked to remove any material deemed to be inappropriate or offensive.

A service provider may be contacted to remove content if the bully refuses or is unable to delete content.

Internet access may be suspended at school for the user for a period of time. Other sanctions for pupils and staff may also be used in accordance to the schools Anti Bullying Policy, Behaviour Policy or Acceptable Use Policy.

Parents/carers will be informed.

The Police will be contacted if a criminal offence is suspected.

Mobile phones and personal device (See Mobile Technology Policy)

The use of mobile phones and other personal devices by students and staff in school will be decided by the school and covered in the Acceptable Use Policy.

The sending of abusive and inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the school community and any breaches will be dealt with as part of the school discipline/behaviour policy.

School staff may confiscate a phone or device if they believe it is being used to contravene the Parklee Community School Behaviour Policy. The phone or device might be searched by the Senior Leadership Team with the consent of the pupil or parent/carer. If there is suspicion that the material on the mobile phone may provide evidence relating to a criminal offence the phone will be handed over to the police for further investigation.

Mobile phones will NOT be used during lessons and formal school time by children or staff. All mobile phones belonging to children will be locked away by the class teacher or supervising adult. Mobile phones belonging to staff will be kept out of the sight of any children.

Mobile phones will NOT be used during after school clubs. All mobile phones will be collected in by the adult at the start of the club and then returned at the end of the session.

Mobile phones will not be used during lessons and formal school time. They should be switched off at all times in line with school policy.

Electronic devices of all kinds that are brought in to school are the responsibility of the user. The school accepts no responsibility for the loss, theft or damage of such items. Nor will the school accept responsibility for any adverse health effects caused by any such devices either potential or actual.Mobile phones and personal devices are not permitted to be used in certain areas within the school site such as changing rooms, toilets or classrooms.

Pupils who bring in mobile phones to school should hand them to the teacher to be locked away for safekeeping until the end of the day.

Pupil Use of Personal Devices

If a pupil breaches the school policy then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents/carers in accordance with the school policy.

If a pupil needs to contact his/her parents/carers they will be allowed to use the school phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office.

Students should protect their phone numbers by only giving them to trusted friends and family members. Students will be instructed in safe and appropriate use of mobile phones and personal devices and will be made aware of boundaries and consequences.

Staff Use of Personal Devices (See Mobile Technology Policy)

Staff are not permitted to use their own personal devices for contacting children, young people and their families within or outside of the setting in a professional capacity.

Staff will need to use the school office phones to contact parents/carers.

Mobile phones and devices will be switched off or switched to ‘silent’ mode, Bluetooth communications should be ‘hidden’ or switched off and mobile phones or devices will not be used during teaching periods unless permission has been given by a member of Senior Leadership Team in emergency circumstances.

Staff should not use personal devices such as mobile phones or cameras to take photos or videos of pupils and will only use work-provided equipment for this purpose.

If a member of staff breaches the school policy then disciplinary action may be taken.

2. Communication Policy

Pupils

All users will be informed that network and internet use will be monitored..

All users (YR-Y6) will be allocated a username and password, with Years 5 and 6 being allowed to choose their own passwords.

An E Safety training programme will be established across the school to raise awareness and importance of safe and responsible internet use amongst pupils.

Pupil instruction regarding responsible and safe use will precede internet access.

An E Safety module will be included in the PSHE, Citizenship and/or Computing programmes covering both safe school and home use.

E Safety training will be part of the transition programmes across the Key Stages.

E Safety rules will be posted in all rooms with Internet access.

Safe and responsible use of the Internet and technology will be reinforced across the curriculum and subject areas.

Particular attention to E Safety education will be given where pupils are considered to be vulnerable.

An E Safety ambassador group will be set up consisting of staff, governors, parent representatives and pupils from across both key stages.

Staff

The E Safety Policy will be formally provided to and discussed with all members of staff.

All staff will be given individual usernames and passwords to access the internet/network.

To protect all staff and pupils, the school will implement Acceptable Use Policies.

Staff will be made aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

Up to date and appropriate staff training in safe and responsible internet use, both professionally and personally, will be provided for all members of staff.

Staff who manage filtering systems or monitor ICT use will be supervised by the Senior Leadership Team and have clear procedures for reporting issues.

The school will highlight useful online tools which staff should use with children in the classroom. These tools will vary according to the age and ability of the children.

All members of staff will be made aware that their online conduct out of school could have an impact on their role and reputation within school. Civil, legal or disciplinary action could be taken if they are found to bring the professional or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

Parents

Parents' attention will be drawn to the school E Safety Policy in newsletters, the school prospectus and the school website.

A partnership approach to E Safety at home and at school with parents will be encouraged.

Parents will be requested to sign an E Safety/Internet agreement as part of the Home School Agreement.

Parents will be encouraged to read the school Acceptable Use Policy for pupils and discuss its implications with their children.

Information and guidance for parents on E Safety will be made available to parents in a variety of formats.

Advice on useful resources and websites, filtering systems, educational and leisure activities which include responsible use of the internet will be made available to parents via the school website.

3. Teaching and Learning - Please read in line with Remote Learning Policy

Internet use is part of the statutory curriculum and is a necessary tool for learning.

The internet is a part of everyday life for education, business and social interaction. The school has a duty to provide students with quality internet access as part of their learning experience.

Pupils use the internet widely outside of school and need to learn how to evaluate internet information and to take care of their own safety and security.

The purpose of internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions.

Internet access is an entitlement for students who show a responsible and mature approach to its use; sanctions will be imposed where Acceptable Use conditions have been breached.

How does Internet use benefit Education?
Benefits of using the Internet in education include:

Access to worldwide educational resources including museums and art galleries.

Inclusions in the National Education Network which connects all UK schools.
Educational and cultural exchanges between pupils worldwide.

Vocational, social and leisure use in libraries, clubs and at home.
Access to experts in many fields for pupils and staff.

Professional development for staff through accession to national developments, educational materials and effective curriculum practice.

Collaboration across networks of schools, support services and professional associations.

Improved access to technical support including remote management of networks and automatic system updates.

Exchange of curriculum and administration data with Wigan Council and DfE.
Access to learning wherever or whenever convenient.

Enhance learning - Please read in line with Remote Learning Policy

Pupils will be taught what internet use is acceptable and what is not and will be given clear objectives for internet use.

Parklee Community School will ensure that the copying and subsequent use of internet derived materials by staff and pupils complies with copyright law.

Access levels to the internet will be reviewed to reflect the curriculum requirement and the age and ability of the pupils.

Staff should guide pupils to online activities that will support the learning outcomes planned for the pupils' age and ability.

Pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.

Pupils will be taught to acknowledge the sources of information used and to respect copyright when using internet material in their own work.

Evaluate Internet Content

Pupils will be taught to critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Pupils will use age-appropriate tools to research internet content.

The evaluation of online materials is a part of teaching and learning in every subject and will be viewed as a whole-school requirement across the curriculum.

4. Managing Information Systems

Information Systems Security

The security of the school information systems and users will be reviewed regularly.

Virus protection will be updated regularly.

Personal data sent over the internet or taken off site should be encrypted. Portable media may not be used without specific permission followed by an

anti-virus/malware scan.
Unapproved software will not be allowed to work in areas or attached to email.

Files held on the school's network will be regularly checked.

The IT Coordinator / Network Manager will review system capacity regularly. The use of user logins and passwords to access the school network will be

enforced.

Email - Please read in line with Remote Learning Policy
Pupils may only use approved email accounts for school purposes.

Pupils must immediately tell a designated member of staff if they receive offensive email (class teacher, SLT or the E Safety Coordinator).

Pupils must not reveal personal details of themselves or other in email communication or arrange to meet anyone without specific permission from an adult.

Staff will only use official school provided email accounts to communicate with parents/carers, as approved by the SLT.

Access in school to external personal email accounts may be blocked.

Excessive social email use can interfere with learning and will be restricted.

Email sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper would be.

The forwarding of chain messages is not permitted.

Staff should not use personal email accounts during school hours or for professional purposes.

Published Content

The contact details on the website should be the school address, email and telephone number. Staff or pupils' personal information must not be published.

The Headteacher will take overall editorial responsibility for online content published by the school and will ensure that content published is accurate and appropriate.

The school website will comply with the school's guidelines for publications including respect for intellectual property rights, privacy policies and copyright.

Pupil's images or work

Images or videos that include pupils will be selected carefully and will not provide material that could be reused.

Pupil's full names will not be used anywhere on the website, particularly in association with photographs.

Written permission from parents or carers will be obtained before images/videos of pupils are electronically published.

Pupils work can only be published with the permission of the parent/carer.

Written consent will be kept by the school where pupils' images are used for publicity purposes, until the image is no longer in use.

The school will have a policy regarding the use of photographic images of children which outlines policies and procedures.

Social Networking, Social Media and Personal Publishing (See Social Media Policy)
Please read in line with Remote Learning Policy

The school will control access to social media and social networking sites.

Pupils will be advised never to give out personal details of any kind which may identify them and or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, instant messaging and email addresses, full names of friends/family, specific interests and clubs etc.

Staff wishing to use social media tools with students as part of the curriculum will risk assess the sites before use and check the sites terms and conditions to ensure the site is age appropriate. Staff will obtain documented consent from the SLT before using social media tools in the classroom.

Staff official blogs or wikis should be password protected and link from the school website with approval from the SLT. Members of staff are advised not to run social networking spaces for pupil use on a personal basis.

Personal publishing will be taught via age appropriate sites that are suitable for educational purposes. They will be moderated by the school where possible.

Pupils will be advised on security and privacy online and will be encouraged to set passwords, deny access to unknown individuals and to block unwanted communications. Pupils will be encourage to approve and invite known friends only on social networking sites and to deny access to others by making profiles private.

All members of the school community are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory. (See Wigan Social Media Policy)

Newsgroups will be blocked unless specific use is approved.

Concerns regarding students' use of social networking, social media and personal publishing sites (in or out of school) will be raised with their parents/carers.

Staff personal use of social networking, social media and personal publishing

sites will be discussed as part of staff induction and safe and professional behaviour will be outlined in the school Acceptable Use Policy.

Filtering (See Technical Security Policy including filtering and Passwords)

The school's broadband access will include filtering appropriate to the age and maturity of pupils.

The school will have a clear procedure for reporting breaches of filtering. All members of the school community (all staff and all pupils) will be aware of this procedure.

If staff or pupils discover unsuitable sites, the URL will be reported in line with the 'responding to incidents of misuse' flow chart.

Any material that the school believes is illegal will be reported to appropriate agencies in line with the above procedures.

The school filtering system (managed by ABtec Computer Solutions Ltd) will block websites that are deemed inappropriate. Staff have permission to ask for websites to be unblocked for educational purposes. Staff will liaise with ABtec Computer Solutions Ltd technicians via the ICT issues book kept in the bursar's office.

Changes to the school filtering policy will be risk assessed by with education and technical experience prior to any changes and where appropriate with consent from the SLT.

The school SLT will ensure that regular checks are made to ensure that the filtering methods selected are effective.

The school's access strategy will be designed by educators to suit the age and curriculum requirements of the pupils, with advice from network managers.

Emerging Technologies – Please read in line with Remote Learning Policy

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

Pupils will be instructed about safe and appropriate use of personal devices both on and off site in accordance with the School Acceptable Use Policy.

Personal Data – please read in line with GDPR Policy.

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1999.