Victoria Park Junior School

E safety policy

March 2020

Victoria Park Junior School
E safety policy

Purpose

The purpose of this policy is to;

- set out the key principles expected of all members of the school community at Victoria Park Junior School with respect to the use of IT-based technologies.
- safeguard and protect the children and staff of Victoria Park Junior School
- assist school staff working with children to work safely and responsibly with the Internet and other communication technologies and to monitor their own standards and practice.
- set clear expectations of behaviour and/or codes of practice relevant to responsible use of the Internet for educational, personal or recreational use.
- have clear structures to deal with online abuse such as online bullying
- ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- minimise the risk of misplaced or malicious allegations made against adults who work with students.

Risks to our school

The main areas of risk for our school community can be summarised as follows:

Content

- exposure to inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence associated with often racist language), substance abuse, lifestyle websites, for example pro-anorexia/self-harm/suicide sites, hate sites, promoting discrimination of any kind, promoting racial or religious hatred;
- content validation: how to check authenticity and accuracy of online content

Contact

- grooming,
- online bullying in all forms,
- identity theft (including 'frape' (hacking Facebook profiles)) and sharing passwords

Conduct

- privacy issues, including disclosure of personal information
- digital footprint and online reputation
- health and well-being (amount of time spent online (Internet or gaming))
- sexting (sending and receiving of personally intimate images) also referred to as SGII (self-generated indecent images)
- extremism copyright (little care or consideration for intellectual property and ownership – such as music and film)

Writing and reviewing the E-safety policy

- The E-Safety Policy is part of the School Development Plan and relates to other policies including those for bullying and for child protection.
- The school's Computing Co-ordinator will also act as E-Safety Coordinator. The E-safety co-ordinate will attend appropriate training and will provide support and training for all staff and volunteers.
- The E-Safety Coordinator will work closely with the Designated Safeguarding Lead as the roles overlap.
- The E-Safety Policy and its implementation will be reviewed annually.
- Any safeguarding concerns, including those related to E-safety are dealt with by the headteacher & DSL (Mrs Taylor) or by the Deputy DSL (mIss Tidman)
- The E-Safety Policy was revised by the E-Safety coordinator and the Headteacher and approved by the Governors in March 2020

Scope (from SWGfL)

This policy applies to all members of Victoria Park Junior School community (including staff, students / pupils, volunteers, governors, parents / carers, visitors, community users) who have access to and are users of Victoria Park Junior School Computing systems, both in and out of Victoria Park Junior School.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of Online bullying, or other Online safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate Online safety behaviour that take place out of school.

Role	Key Responsibilities
Headteacher	• To take overall responsibility for Online Safety provision • To ensure the school uses an approved, filtered Internet Service, which complies with current statutory requirements • To be responsible for ensuring that staff receive suitable training to carry out their Online safety roles. • To be aware of procedures to be followed in the event of a serious E-safety incident. • To receive regular monitoring reports from the E-safety Safety Co-ordinator.

E-safetyy Co-ordinator / Computing Coordinator	• Takes day to day responsibility for Online safety issues and has a leading role in establishing and reviewing the school Online safety policies / documents
	• Promotes an awareness and commitment to Online safeguarding throughout the school community
	• Ensures that Online safety education is embedded across the curriculum
	• Liaises with school Computing technical staff
	• Liaise any issues with Designated Safeguarding Lead.
	• To communicate with SLT to discuss any issues and review any incident logs.
	• To ensure that all staff are aware of the procedures that need to be followed in the event of an Online Safety incident
	• To ensure that an Online safety incident log is kept up to date
	• Facilitates training and advice for all staff
	• Liaises with the Local Authority and relevant agencies
	• Is regularly updated in E-safety issues and legislation, and be aware of the potential for serious child protection issues to arise from:
	  • sharing of personal data
	  • access to illegal / inappropriate materials
	  • inappropriate on-line contact with adults / strangers
	  • potential or actual incidents of grooming
	  • Online bullying and use of social media

Governors	• To ensure that the school follows all current Online safety advice to keep the children and staff safe • To approve the E-Safety Policy and review the effectiveness of the policy.
Network technicians	• To report any online safety related issues that arise, to the E- safety coordinator. • To ensure that users may only access the school's networks through an authorised and properly enforced password protection policy, in which passwords are regularly changed • To ensure that provision exists for misuse detection and malicious attack e.g. keeping virus protection up to date) • To ensure the security of the school IT system • To ensure that access controls / encryption exist to protect personal and sensitive information held on school-owned devices • The school's policy on web filtering is applied and updated on a regular basis • that the use of the *network/ email* is regularly monitored in order that any misuse / attempted misuse can be reported to the E-Safety co-ordinator / Head teacher for investigation. • To ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster. • To keep up-to-date documentation of the school's online security and technical procedures.

Role	Key Responsibilities
Teachers	• To embed online safety issues in all aspects of the curriculum and other school activities • To supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant) • To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws
All staff	• To read, understand and help promote the school's e-safety policies and guidance • To read, understand, sign and adhere to the school staff Acceptable Use Agreement / Policy • To be aware of online safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices • To report any suspected misuse or problem to the E safety coordinator or SLT • To maintain an awareness of current online safety issues and guidance. • To model safe, responsible and professional behaviours in their own use of technology • To ensure that any digital communications with pupils should be on a professional level and only through school based systems, never through personal mechanisms, e.g. email, text, mobile phones etc. • All staff have a responsibility to report any Esafety issues to the relevant persons. Reports should be passed to SLT and where necessary to relevant agencies • It is important that all staff are responsible for their own actions but also for monitoring and reporting worrying actions witnessed by other members of staff to ensure the safety of all children and staff within school.
Pupils	• Read, understand, and adhere to Computer rules. • Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations • To understand the importance of reporting abuse, misuse or access to inappropriate materials • To know what action to take if they or someone they know feels worried or vulnerable when using online technology. • To know and understand school policy on the use of mobile phones, digital cameras and hand held devices. • To know and understand school policy on the taking / use of images and on cyber-bullying. • To understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's E- Safety Policy covers their actions out of school, if related to their membership of the school • To take responsibility for learning about the benefits and risks of using the Internet and other technologies safely both in school and at home • To help the school in the creation/ review of E-safety policies
Parents/carers	• To support the school in promoting online safety. • To read, understand and promote the school Pupil Computer rules (found in the school diary) with their children • To consult with the school if they have any concerns about their children's use of technology.
External groups	• Any external individual / organisation will sign an Acceptable Use Policy prior to using any equipment or the Internet within school

Teaching and learning

Why Internet use is important
The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide children with quality Internet access as part of their learning experience. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

Internet use will enhance learning
The school Internet access is designed expressly for pupil use and includes filtering appropriate to the age of pupils. Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use. 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 how to evaluate Internet content
The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law. Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Every year there will be a Safer Internet Day, during which children will discuss e-safety and the relevant areas in relation to this at an appropriate level for their age group. They will be expected to engage with and produce learning which helps them to understand how to keep themselves safe when using technology within and outside of school.

In order for staff to deliver e-safety coverage, they are frequently trained on E-safety. At least once a year, staff receive e-safety training. Staff are made aware of practices, procedures, relevant information and where to find additional resources or information to further their knowledge.

Managing internet use

Information system security
- School ICT systems capacity and security will be reviewed regularly through conversations between senior leadership, computing co-ordinator, network technicians and the governors.
- Virus protection will be updated regularly.
- The security of the school network relies on the central firewall implemented by Trafford MBC. No traffic shall enter or leave the TMBC Infrastructure without being explicitly permitted by the firewall. No traffic shall route directly between connected establishments unless it has been explicitly allowed to do so. The configuration of the firewall can be changed at the request of the school when a security review will be conducted and advice taken from TMBC.
- Websites are only accessed through Proxy Servers provided by Trafford.
- Password security is of the utmost importance and must be maintained at all times. Adults and children will be reminded never to disclose their passwords. The abuse of passwords must be reported immediately to the E-Safety coordinator.
- All children have their own individual log in accounts for school computer access and their history is checked on a regular basis.

In addition to this, users may also not use the school's internet services in the following manners or instances:
- To run a private business

- Visit sites which may be defamatory or incur liability or adversely impact upon the image or reputation of the school
- Use, upload, download or transmit copyrighted material
- Reveal confidential information, which includes but is not limited to: financial information, personal information, databases, computing access codes, business relationships.
- Use the internet to reveal personal opinions which could be considered inappropriate or offensive
- Violate the privacy of others
- Corrupting or deleting others' data within prior permission
- Continue to use a device or item after request to desist because it is causing technical, safety, privacy or other issues
- Use technologies to intimidate, threaten or cause harm to others

Managing filtering

- Developing good practice in internet use as a tool for teaching and learning is essential. School internet access will be designed for pupil and teaching use and will include filtering policies appropriate to the age of the children.
- The school will work with the TMBC, DfE and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
- No filtering system is perfect and pupils (and staff) will be taught what to do if they experience material they find distasteful, uncomfortable or threatening. This will be recorded in the e-Safety log and reported to the E-Safety Coordinator and the URL and content will be reported to the TMBC ICT service team.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- Change requests, to allow or block sites, will be made to the ICT service desk.

On-line working and communication

- The school will control access to moderated social networking sites and educate pupils in their safe use.
- Our policy is to block/filter access to other social networking sites such as 'Twitter, Facebook' or 'Instagram' and to chat rooms. (Most have a minimum age of 13 specified).
- Pupils will be taught the importance of personal safety when using social networking sites and chat rooms. They will be advised never to give out personal details of any kind which may identify them or their location.
- Pupils will be taught to consider the thoughts and feelings of others when publishing material to websites and elsewhere. Material or comments which may be perceived to victimise or bully someone, or is otherwise offensive, is unacceptable and appropriate sanctions will be implemented.
- Any misuse will be recorded in the E-Safety log. This will include online activity carried out outside of school.
- Staff will not exchange personal social networking addresses or use social networking sites to communicate directly with pupils.
- Pupils and parents will be advised about inappropriate use of social network spaces outside school.
- There is information available for both children and parents in regards to online safety listed on the school website.

E-mail and other communications systems

Pupils

Pupils may only use approved, teacher supervised, e-mail accounts

Pupils are taught;

- That personal e-mail or messaging between staff and pupils/parents should not take place. To be appropriate, sensible and responsible use of e-mail.
- About the online safety and 'netiquette' of using e-mail both in school and at home.
- Not to share their e-mail address
- That they must not reveal person details of themselves or others in e mail.
- To 'Stop and Think Before They Click' and not open attachments unless sure the source is safe;
- To think carefully before sending any attachments
- To immediately tell a teacher / responsible adult if they receive an e-mail which makes them feel uncomfortable, is offensive or bullying in nature
- Not to respond to malicious or threatening messages;
- Not to delete malicious of threatening e-mails, but to keep them as evidence of bullying;
- Not to arrange to meet anyone they meet through e-mail without having discussed with an adult and taking a responsible adult with them.

Staff / parents / carers

- Communication between school and parents will be via telephone, letter and face to face. Staff must only use their school email address for professional use and makes clear personal email should be through a separate account.
- Does not publish personal e-mail addresses of pupils or staff on the school website.
- Will contact the Police if one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law.
- Reports messages relating to or in support of illegal activities to the relevant Authority and if necessary to the Police.
- Knows that spam, phishing and virus attachments can make e mails dangerous. We use a number of technologies to help protect users and systems in the school, including desktop anti-virus product Sophos.

Published content and the school web site

- Editorial guidance will ensure that the school's ethos is reflected in the website, information is accurate, well presented and personal security is not compromised. Care will be taken to ensure that all information is considered from a security viewpoint including the use of photographic material.
- The contact details on the Web site should be the school address, e-mail and telephone number.
- Staff or pupils' personal information will not be published.
- The headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.
- Photographs, videos and podcasts of school activities, alongside first names only, may be uploaded. This is inline with what may be shown on a classroom wall or school display and shared within our physical community.
- Pupil work may be displayed that whilst commendable, may not be of a normal publishable standard.

Publishing pupil's images and work

- Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified by members of the public viewing the website.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.
- Pupil's work can only be published with the permission of the pupil and parents.
- The permissions will be requested from parents on initial entry to the school.

Managing emerging technologies

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

Protecting personal data

Personal data will be recorded, processed, transferred and made available according to GDPR

Password policy

- This school makes it clear that staff and pupils must always keep their password private, must not share it with others and must not leave it where others can find it;
- All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password private.
- We encourage staff to use strong passwords and regularly change their passwords.

Equipment and Digital Content

Personal mobile phones and mobile devices

- Mobile phones brought into school are entirely at the staff member, Pupil's & parents' or visitors own risk. The School accepts no responsibility for the loss, theft or damage of any phone or hand held device brought into school.
- Staff will be issued with a school phone where contact with parents is required and will not use or disclose personal phone numbers.
- All visitors are requested to keep their phones on silent.
- The recording, taking and sharing of images, video and audio on any mobile phone is not permitted.
- Where parents or students need to contact each other during the school day, they should do so only through the School's telephone.
- Mobile phones and personally-owned devices will not be used in any way during lessons. They should be switched off or silent at all times.
- The Bluetooth / Airplay or similar function of a mobile phone should be switched off at all times and not be used to send images or files to other mobile phones or handheld devices.
- Staff are not allowed to connect any of their personal devices to the school's Wi-Fi network or server

Pupils' use of personal devices

- The School strongly advises that student mobile phones should not be brought into school.
- Mobile phones will be discouraged in school, if brought in they will be held in the office until the end of the day.

- The School accepts that there may be particular circumstances in which a parent wishes their child to have a mobile phone for their own safety.
- If a student 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 or carers in accordance with the school policy.
- Children are not allowed to take videos or photographs using their mobile devices on school property.

Parents/ carers

- Parents are politely requested to leave their phone out of sight and refrain from answering any phone calls whilst inside the school building.
- Parents are asked to set their phone to silent mode during any events
- Photographs and video footage can be taken of their own child under GDPR, as long as it is only of their child and for their personal viewing only. Parents are reminded that they should not post photographs or video footage of other children without their prior consent on social media sites at every event.
- Parents are reminded about when they can take photos and videos and that they should only be of their child at the relevant events. It is also explained that they should not be used to show other children on social media sites.
- Parents are not permitted to use any technologies that belong to the school without staff supervision.

Policy decisions

- All staff must read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource.
- The school will keep a record of all staff and pupils who are granted Internet access.
- The record will be kept up-to-date, for instance, a member of staff may leave or a pupil's access be withdrawn.
- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer.
- The school cannot accept liability for the material accessed, or any consequences of Internet access.
- The school will audit ICT provision to establish if the E-safety policy is adequate and that its implementation is effective.