WEST PARK ACADEMY
E-Safety Policy

Reviewed: February 2024

WEST PARK ACADEMY
E-SAFETY POLICY

CONTENTS

INTRODUCTION

The purpose of the West Park Academy E-Safety Policy is to:

- Clearly identify the key principles expected of all members of the community with regards to the safe and responsible use of technology to ensure that West Park Academy is a safe and secure environment
- Safeguard and protect all members of the West Park Academy community online
- Raise awareness with all members of the West Park Academy community regarding the potential risks as well as benefits of technology
- To enable all staff to work safely and responsibly, to role model positive behaviour online and be aware of the need to manage their own standards and practice when using technology
- Identify clear procedures to use when responding to online safety concerns that are known by all members of the community

This policy applies to all staff including the board of trustees, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for or provide services on behalf of the school (collectively referred to as 'staff' in this policy) as well as children and parents/carers.

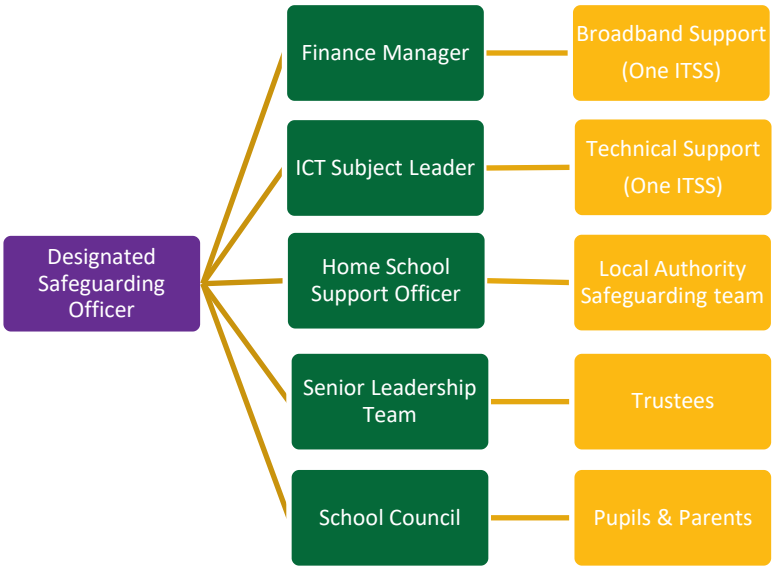
This policy applies to all who have access to the internet and use of information communication devices, including personal devices, or where children, staff or other individuals have been provided with school issued devices for use off-site, such as a work laptops, tablets or mobile phones.

This policy must be read in conjunction with other relevant school policies which are detailed in West Park Academy's Safeguarding and Child Protection Policy. These include but are not limited to safeguarding and child protection, anti-bullying, behaviour, Acceptable Use Policies, confidentiality and relevant curriculum policies including Computing and Personal Social and Health Education.

E-SAFETY ROLES

WHO WILL WRITE AND REVIEW THE POLICY?

- The Academy Designated Safeguarding Lead with take the role of Lead E-Safety officer but will work closely with the ICT Subject Leader to develop policies and ensure a relevant curriculum is in place
- The E–Safety Policy and its implementation will be reviewed annually by the E-Safety Committee detailed below
- E-Safety Committee detailed below will ensure that the policy review and E-Safety monitoring is completed



TEACHING AND LEARNING

How Will Internet Safety Be Taught To Pupils?

- An online safety (Digital Literacy) curriculum will be established and embedded throughout the whole school, to raise awareness regarding the importance of safe and responsible internet use amongst pupils
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy and this is done through Digital Literacy lessons
- Online safety (E-Safety) will be included in the PSHE, SRE, Citizenship and Computing programmes of study, covering both safe school and home use

How Will Staff Be Trained?

- The online safety (E-Safety) policy will be formally provided to and discussed with all members of staff as part of induction and will be reinforced and highlighted as part of our safeguarding responsibilities
- Staff will be made aware that our Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential when using school systems and devices
- 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 in a variety of ways, on a regular (at least annual) basis
- 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 profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities
- Members of staff with a responsibility for managing filtering systems or monitor ICT use will be supervised by the Leadership Team and will follow the Code of Conduct if there is need to report concerns

TECHNICAL INFORMATION

HOW WILL INFORMATION SECURITY SYSTEMS BE MAINTAINED?

- The security of the school information systems and users will be reviewed regularly
- Virus protection will be updated regularly
- The academy will deploy monitoring software to track computer and internet use. This software will include keyword detection and incident logging
    - Keyword detection includes, but is not limited to:
        - Adult content
        - Anti-bullying & online 'trolling'
        - Counter radicalisation, extremism & terrorism
        - Eating disorders
        - Grooming
        - Homophobic language
        - Racist language
        - Self-harm
        - Sexting
        - Suicide
- The academy will ensure that systems to protect pupils are reviewed and improved
- If staff or pupils discover unsuitable sites, the URL must be reported to the E–Safety Coordinator via email or through CPOMS
- The school's broadband access will include filtering appropriate to the age and maturity of pupils
- The academy Designated Safeguarding Lead will work in collaboration with the ICT Lead and the ICT Support team (One ITSS) to ensure that filtering and monitoring systems are in place and reviewed regularly. Filtering systems will be maintained and configured following advice from "Keeping Safe In Education 2023" and the "Meeting digital and technology standards in schools and colleges" documentation.

How Will Email Be Managed?

- Pupils may only use approved email accounts which are set up to accept internal mail only
- Pupils must immediately tell a teacher if they receive offensive email from another user
- Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission from an adult
- Whole-class or group email addresses will be used in primary schools for communication outside of the school
- Staff email use is governed by the Staff Acceptable Use Policy in conjunction with the latest Code of Conduct for staff
- Should staff use personal devices to access Academy Email the device **must** be password protected and **no data** should be saved to that device
- For staff email accounts (Office 365) two factor authentication is set up when accessing off the school site or on a mobile device

How Will Published Content Be Managed?

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

Can Pupils' Images Or Work Be Published?

- Images that include pupils will be selected carefully and will not provide material that could be reused
- Pupils' full names should not be used on the website, particularly in association with photographs
- Written permission from parents or carers will be obtained before images of pupils are electronically published
- Pupils work can only be published with their permission

How Will Social Networking, Social Media and Personal Publishing Be Managed?

- The academy will control access to social media and social networking sites and in most cases these websites are blocked by our filtering system
- 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, IM and email addresses, full names of friends/family, specific interests and clubs

- As part of Digital Literacy lessons children are made aware of the benefits and potential risks with social media. They will also be made aware of age ratings for social media sites.

How Should Personal Data Be Protected?

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018 and governed through GDPR regulations 2018
- This is governed through the Staff ICT Acceptable Use Policy and Code of Conduct in relation to taking sensitive information offsite

How Will Internet Access Be Authorised?

- The school will maintain a current record of all staff and pupils who are granted access to the school's electronic communications
- All staff must read and sign the Staff Acceptable Use form
- At Key Stage 1, access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials
- Parents and Pupils will be asked to sign and return a Pupil Acceptable Use form

How Will Risks Be Assessed?

- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. The school cannot accept liability for the material accessed, or any consequences resulting from Internet use
- Children are taught to be critically aware of the websites and information they access using the Internet. There are reporting procedures in place to deal with any of these instances. This is re-enforced with the pupils during E-Safety lessons
- The school will audit ICT use to establish if the E–Safety policy is adequate and that the implementation of the E–Safety policy is appropriate

E-SAFETY INCIDENT REPORTING

How Will E-Safety Incidents Be Handled?

- Instances of Internet misuse will first be reported to the ICT co-ordinator who will then refer these to the Principal. The Principal will then deal with this as per the Safeguarding and Child Protection Policy.
- Any complaint about staff misuse must be referred to the Principal. This will then be dealt with as per Employee Code of Conduct
- E–Safety complaints and incidents will be recorded by the school using Cpoms, the Academy's system for logging bullying, safeguarding and behaviour issues
- Children may log an incident by speaking to their class teacher or any other staff member. They can also report issues or concerns through the Confide button on all computers across the Academy. There is also the email inbox confide@westparkacademy.org.uk. This gives pupils the opportunity to report any incidents themselves but it also timestamps and details all interactions and responses to an incident
- Once logged through email, Confide or through a staff member the information will be recorded on Cpoms and any actions will be documented.

How Will Cyber Bullying Be Managed?

- Cyberbullying (along with all forms of bullying) will not be tolerated in school. Full details are set out in the school's policy on anti-bullying
- There will be clear procedures in place to support anyone effected by Cyberbullying.
- Staff can log incidents through Cpoms or contact the Designated Safeguarding Lead directly, who will then log the incident on Cpoms or direct to the relevant body
- The Academy will be sensitive to Internet related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice

Digital Learning Environments

How Will Digital Learning Be Managed?

- SLT and staff will monitor the usage of the Microsoft Teams / Office 365 by pupils and staff regularly in all areas, in particular message and communication tools and publishing facilities
- Pupils/staff will be advised on acceptable conduct and use when using the Microsoft Teams / Office 365.
- Only pupils and members of the staff community will have access to Microsoft Teams / Office 365 groups.
- All users will be mindful of copyright issues and will only upload appropriate content onto Microsoft Teams / Office 365.

- When staff, pupils etc leave the school their account or rights to specific school areas will be disabled or transferred to their new establishment if applicable

POLICY REVIEW

HOW WILL THE POLICY BE INTRODUCED TO PUPILS?

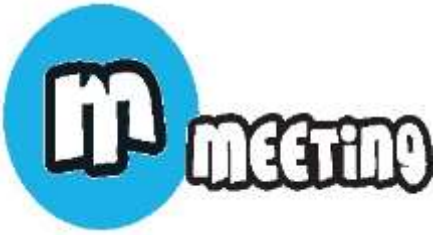
- All users will be informed that network and Internet use will be monitored
- An E–Safety scheme of work titled 'Digital Literacy' has been introduced to raise the awareness and importance of safe and responsible internet use
- Children will be introduced to the school Internet Rules (Smart Rules) see appendices and are required to sign and return a Pupil Acceptable Use Policy, this is monitored and a record is kept by admin staff
- Assemblies will take place throughout the year to re-enforce our E-Safety messages.

HOW WILL PARENTS SUPPORT BE ENLISTED?

- Parents' attention will regularly be drawn to the School E–Safety Policy in newsletters and on the school website
- Updates are sent to parents periodically throughout the year through newsletters and parent workshops
- The Academy will endeavour to improve parental engagement through the usual academy communication channels

SCHOOL INTERNET RULES

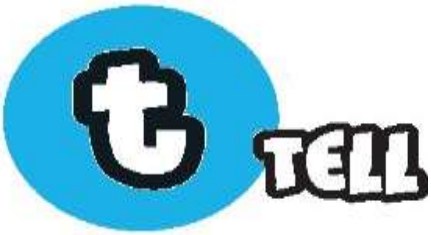
- I will not deliberately use the computers to try and find any material that might upset me, or other children or adults
- If I am found using the Internet to find unsuitable material I will be banned from using the Internet for a period of time and my parents / guardians will be told
- I will stay **safe** by never telling anyone my real name, address, phone number or school when I am using the Internet



- I will never **meet**, or arrange to **meet**, anyone I meet on the Internet or by email or messaging

- I will only send or **accept** an email or message with permission and when there is an adult with me
- I will only send emails to an address I know and I will always use polite language

- I will only use the Internet for schoolwork, with adult permission and when an adult is with me
- I know that some information might not be **reliable** and I will check with an adult if I am unsure



- I will not copy other people's work without **telling** them and getting their permission first
- If I find anything that upsets me on the Internet, I will turn off the monitor straight away and **tell** an adult
- I know that teachers will be able to **tell** what I have been looking at on the Internet by checking the history list of websites
- I will not alter, change or delete any of the settings and files on the computers unless I have permission. I will **tell** an adult if I do this by accident

Written: September 2013 (D Fraser)

Reviewed: September 2014 (D Fraser)
March 2016 (D Fraser)
October 2016 (D Fraser and H Dummett)*
*Reviewed October 2016 due to update to Keeping Children Safe in Education guidance issued September 2016.
December 2017 (D Fraser)
January 2019 (D Fraser)
January 2020 (D Fraser)
January 2021 (D Fraser)
December 2021 (D Fraser)
February 2023 (D Fraser)
February 2024 (D Fraser)

Next Review Date: February 2025
**Review date amended to ensure any further changes to policy and practices are addressed on an annual basis