E-Safety Policy

(September 2019)

Park Community School

Document Control Table	
Associated documents	Safeguarding Policy Behaviour Policy
Date approved by Governors	25/09/2019
Date of review	September 2020

Contents

1 Scope of the Policy

This policy applies to all members of Park Community School (including staff, students, volunteers, parents / carers, visitors, community users) who have access to and are users of school digital technology systems, both in and out of the school.

The Education and Inspections Act 2006 empowers headteachers, to such extent as is reasonable, to regulate the behaviour of students 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 E-Safety incidents covered by this policy, which may take place outside of Park Community School, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

Park Community 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 E-Safety behaviour that take place out of school.

2 Roles and Responsibilities

The following section outlines the E-Safety roles and responsibilities of individuals and groups within the school:

(a) Governors

The Governing Body is responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governing Body receiving regular information about online safety incidents and monitoring reports. A member of the Governing Body has taken on the role of E-Safety Governor (Barry Harwood). The role of the E-Safety Governor will include:

- regular meetings with the E-Safety Co-ordinator
- attendance at E-Safety Group meetings
- regular monitoring of online safety incident logs
- regular monitoring of filtering / change control logs
- reporting to relevant Governors meeting

(b) Headteacher and Senior Leaders

- The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the E-Safety Lead.
- The Headteacher and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
- The Headteacher and Senior Leaders are responsible for ensuring that the E-Safety Lead and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Headteacher and Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

- The Senior Leadership Team will receive regular monitoring reports from the E-Safety Lead.

(c) E-Safety Lead

The E-Safety Lead will:

- lead the E-Safety Group
- take day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies and documents
- ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- provide training and advice for staff
- liaise with outside agencies
- liaise with school technical staff
- receive reports of online safety incidents and create a log of incidents to inform future online safety developments,
- meet with the E-Safety Governor to discuss current issues, review incident logs and filtering / change control logs
- report annually to the Governing Body
- report regularly to Senior Leadership Team

(d) Network Manager

The Network Manager is responsible for ensuring:

- that the school's 's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets required online safety technical requirements and any Local and other relevant body E-Safety Guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- the filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- that the use of the network / internet / Learning Platform / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher or other Senior Leader; E-Safety Lead for investigation and sanction
- that monitoring software systems are implemented and updated as agreed in school policies

(e) Teaching and Support Staff

Are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current school E-Safety Policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP) – see Appendix 2.
- they report any suspected misuse or problem to the Headteacher or Senior Leader or E-Safety Lead for investigation
- all digital communications with students / parents / carers should be on a professional level and only carried out using official school systems
- online safety issues are embedded in all aspects of the curriculum and other activities
- students understand and follow the E-Safety Policy and acceptable use policies
- students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations

- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

(f) Designated Safeguarding Lead

Should be trained in E-Safety issues and be aware of the potential for serious child protection and safeguarding issues to arise from:

- sharing of personal data
- access to illegal or inappropriate materials
- inappropriate online contact with adults or strangers
- potential or actual incidents of grooming
- online-bullying

(g) Students

- are responsible for using the school's digital technology systems in accordance with the Student Acceptable Use Agreement contained in the 'Moving Up' pack
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking and use of images and on online-bullying.
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's 's E-Safety Policy covers their actions out of school, if related to their membership of the school

(h) Parents and Carers

Parents and carers play a crucial role in ensuring that their children understand the need to use the internet and mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national / local online safety campaigns / literature. Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website and online student records
- their children's personal devices in the school (where this is allowed)

(i) Community Users

Community Users who access school systems/website as part of the wider school provision will be expected to sign a Community User AUA (see Appendix 3) before being provided with access to school systems.

3 Online Safety and Social Media

(a) Overview

With the current speed of on-line change, some parents and carers have only a limited understanding of online risks and issues. Parents may underestimate how often their children come

across potentially harmful and inappropriate material on the internet and may be unsure about how to respond. Some of the risks could be:

- unwanted contact
- grooming
- online bullying including sexting
- digital footprint

The school will therefore seek to provide information and awareness to both pupils and their parents through:

- Acceptable use agreements for children, teachers, parents/carers and governors
- Curriculum activities involving raising awareness around staying safe online
- Information included in letters, newsletters, web site, VLE
- Parents evenings / sessions
- High profile events / campaigns e.g. Safer Internet Day
- Building awareness around information that is held on relevant web sites and or publications
- Social media policy
- Where rules are broken or concerns caused the school may take action. Action may be at a school leader level or via other organisations including the police.

(b) Cyberbullying

Central to the school's anti-bullying policy is the principle that '*bullying is always unacceptable*' and that '*all pupils have a right not to be bullied*'.

The school also recognises that it must take note of bullying perpetrated outside school which spills over into the school; therefore once aware we will respond to any cyber-bullying we become aware of carried out by pupils when they are away from the site.

Cyber-bullying is defined as 'an aggressive, intentional act carried out by a group or individual using electronic forms of contact repeatedly over time against a victim who cannot easily defend himself/herself.'

By cyber-bullying, we mean bullying by electronic media:

- Bullying by texts or messages or calls on mobile 'phones
- The use of mobile 'phone cameras to cause distress, fear or humiliation
- Posting threatening, abusive, defamatory or humiliating material on websites, to include blogs, personal websites, social networking sites
- Using e-mail to message others
- Hijacking/cloning e-mail accounts
- Making threatening, abusive, defamatory or humiliating remarks in on-line forums

Cyber-bullying may be at a level where it is criminal in character. It is unlawful to disseminate defamatory information in any media including internet sites.

Section 127 of the Communications Act 2003 makes it an offence to send, by public means of a public electronic communications network, a message or other matter that is grossly offensive or one of an indecent, obscene or menacing character.

The Protection from Harassment Act 1997 makes it an offence to knowingly pursue any course of conduct amounting to harassment.

If we become aware of any incidents of cyberbullying, we will need to consider each case individually as to any criminal act that may have been committed. The school will pass on information to the police if it feels that it is appropriate or is required to do so.

(c) Sexting

'Sexting' often refers to the sharing of naked or 'nude' pictures or video through mobile phones and/or the internet. It also includes underwear shots, sexual poses and explicit text messaging. While sexting often takes place in a consensual relationship between two young people, the use of sexted images in revenge following a relationship breakdown is becoming more commonplace. Sexting can also be used as a form of sexual exploitation and take place between strangers.
As the average age of first smartphone or camera enabled tablet is 6 years old, sexting is an issue that requires awareness raising across all ages.

The school will use age appropriate educational material to raise awareness, to promote safety and deal with pressure. Parents should be aware that they can come to the school for advice.

(d) Gaming

Online gaming is an activity in which the majority of children and many adults get involved. The school will raise awareness:

- By talking to parents and carers about the games their children play and help them identify whether they are appropriate
- By supporting parents in identifying the most effective way to safeguard their children by using parental controls and child safety mode
- By talking to parents about setting boundaries and time limits when games are played
- By highlighting relevant resources.

(e) Online reputation

Online reputation is the opinion others get of a person when they encounter them on-line. It is formed by posts, photos that have been uploaded and comments made by others on people's profiles. It is important that children and staff are aware that anything that is posted could influence their future professional reputation. The majority of organisations and work establishments now check digital footprint before considering applications for positions or places on courses.

(f) Grooming

On-line grooming is the process by which one person with an inappropriate sexual interest in children will approach a child on-line, with the intention of developing a relationship with that child, to be able to meet them in person and intentionally cause harm.

The school will build awareness amongst children and parents about ensuring that the child:

- Only has friends on-line that they know in real life
- Is aware that if they communicate with somebody that they have met on-line, that relationship should stay on-line.

That the school will support parents to:

- Recognise the signs of grooming

- Have regular conversations with their children about on-line activity and how to stay safe on-line

The school will raise awareness by:
- Running sessions for parents
- Include awareness around grooming as part of their curriculum
- Identifying with parents and children how they can be safeguarded against grooming.

4 Policy Statements

(a) Education – Students

Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students in online safety and digital literacy is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:
- A planned online safety curriculum should be provided as part of Computing, PD and other relevant lessons and should be regularly revisited
- Key online safety messages should be reinforced as part of a planned programme of assemblies.
- Students should be taught in all lessons to be critically aware of the materials / content they access online and be guided to validate the accuracy of information.
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Students should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.
- Students should be helped to understand the need for the student/pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school.
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices
- in lessons where internet use is pre-planned, it is best practice that students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where students are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

(b) Education – Parents /Carers

Parents and carers may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.
The school will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters, web site, MyEd
- Parents' /Carers' evenings
- High profile events and campaigns e.g. Safer Internet Day

(c) Education & Training – Staff /Volunteers

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school E-Safety Policy and Acceptable Use Agreements.
- It is expected that some staff will identify online safety as a training need within the performance management process.
- The E-Safety Lead will receive updates through training events and by reviewing guidance documents released by relevant organisations.
- This E-Safety Policy and its updates will be presented to and discussed by staff in relevant meetings.
- The E-Safety Lead (or other nominated person) will provide advice and guidance to individuals as required.

(d) Training – Governors/Directors

Governors should take part in online safety training and awareness sessions. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority/National Governors Association/or other relevant organisation
- Participation in school training / information sessions for staff or parents

Appendix 1 - Development / Monitoring / Review of this Policy

This E-Safety policy has been developed by a working group made up of:

- Headteacher and Senior Leaders
- E-Safety Coordinator
- Staff – including Teachers, Support Staff, Technical staff
- Governors
- Parents and Carers
- Community users

Consultation with the whole school community has taken place through a range of formal and informal meetings.

Schedule for Development / Monitoring / Review

This E-Safety policy was approved by the Governing Body on:	25/09/2019
The implementation of this E-Safety policy will be monitored by the:	Senior Leadership Team
Monitoring will take place at regular intervals:	At least once a year
The Governing Body will receive a report on the implementation of the E-Safety Policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals:	At least once a year
The E-Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	May 2020
Should serious online safety incidents take place, the following external persons / agencies should be informed:	LA Safeguarding Officer, Police

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited) / filtering
- Internal monitoring data for network activity
- Surveys / questionnaires of
    - students
    - parents / carers
    - staff

Appendix 2 - Staff and Volunteer Acceptable Use Agreement

New technologies have become integral to the lives of children and young people in today's society, both within schools / academies and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe access to the internet and digital technologies at all times.

This Acceptable Use Policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications 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 users at risk.
- that staff are protected from potential risk in their use of technology in their everyday work.

The school will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities for students learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement
I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that students / pupils receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

For my professional and personal safety:

- I understand that the school / academy will monitor my use of the school digital technology and communications systems.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email, VLE etc.) out of school, and to the transfer of personal data (digital or paper based) out of school
- I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- 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 immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using school ICT 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 when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / 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 (eg on the school website / VLE) 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.

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

- When I use my mobile devices (laptops / tablets / mobile phones / USB devices etc) in school, I will follow the rules set out in this agreement, 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 use personal email addresses on the school ICT systems.
- 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 ensure that my data is regularly backed up, in accordance with relevant school / academy policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist 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 try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- 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.
- I will not disable or cause any damage to school / academy 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 / 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 Protected and Restricted data must be held in lockable storage.
- I understand that data protection policy requires that any staff or student / pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school / academy 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 the school / academy:
- I understand that this Acceptable Use Policy applies not only to my work and use of school / academy digital technology equipment in school, but also applies to my use of school /

academy systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school / academy

- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could a warning, a suspension, referral to Governors and the Local Authority and in the event of illegal activities the involvement of the police.

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.

Staff / Volunteer Name: ……..

Signed: …… Date: ……

Appendix 3 – Community Users Acceptable Use Agreement

This Acceptable Use Agreement is intended to ensure:

- that community users of school digital technologies will be responsible users and stay safe while using these systems and devices
- that school systems, devices and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that users are protected from potential risk in their use of these systems and devices

Acceptable Use Agreement

I understand that I must use school systems and devices in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems, devices and other users. This agreement will also apply to any personal devices that I bring into the school:

- I understand that my use of school systems and devices and digital communications will be monitored
- I will not use a personal device that I have brought into school for any activity that would be inappropriate in a school setting.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist 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 immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.
- I will not access, copy, remove or otherwise alter any other user's files, without permission.
- I will ensure that if I take and / or publish images of others I will only do so with their permission. I will not use my personal equipment to record these images, without permission. If images are published it will not be possible to identify by name, or other personal information, those who are featured.
- I will not publish or share any information I have obtained whilst in the school on any personal website, social networking site or through any other means, unless I have permission from the school.
- I will not, without permission, make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a school device, nor will I try to alter computer settings, unless I have permission to do so.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will immediately report any damage or faults involving equipment or software; however, this may have happened.
- 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 if I fail to comply with this Acceptable Use Agreement, the school has the right to remove my access to school systems / devices

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.

Name: ..... Signed: .....

Date: .....