Parklands Community Primary & Nursery School

E-Safety Policy

March 2022

The member of school responsible for e-safety is Laura Hughes

All members of the school community should agree to an Acceptable Use Policy that is appropriate to their age and role.

Appendix 1: Acceptable Use Policy for Staff & Governors
Appendix 2: Acceptable Use Policy for KS1 and KS2
*The AUP will form part of the first lesson of computing for each year group.
Appendix 2: AUP sent to parents/home school agreement
Appendix 3: Switched on Computing - Guide for using the internet safely
Appendix 4: One-page document on Remote/Blended learning
Appendix 5: One-page summary of the e-Safety Policy

Introduction

ICT is an essential resource to support learning as playing an important role in the everyday lives of children, young people and adults. Consequently, Parklands Community Primary School needs to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment while maintaining their own safety online. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Virtual Learning Platforms
- Email and Instant Messaging
- Chat Rooms and Social Networking
- Forums, Wikis and Blogs
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices with web functionality

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies.

We understand the responsibility to educate our pupils on eSafety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

The Prevent Duty

The Prevent Duty is the duty in the Counter-Terrorism and Security Act 2015 on specified authorities (Schools) in the exercise of their functions, to have due regard to the need to prevent people from being drawn into terrorism.

The general risks affecting children and young people may vary from area to area, and according to their age. Schools and childcare providers are in an important position to identify risks within a given local context.

Schools and childcare providers should be aware of the increased risk of online radicalisation, as organisations seek to radicalise young people through the use of social media and the internet.

The statutory guidance makes clear the need for schools to ensure that children are safe from terrorist and extremist material when accessing the internet in schools. Schools should ensure that suitable filtering is in place.

More generally, schools have an important role to play in equipping children and young people to stay safe online, both in school and outside. Internet safety will usually be integral to a school's Computing curriculum and can also be embedded in PSHE and SRE. General advice and resources for schools on internet safety are available on the UK Safer Internet Centre website. As with other online risks of harm, all staff needs to be aware of the risks posed by the online activity of extremist and terrorist groups.

The Prevent Duty means that all staff have a duty to be vigilant and where necessary report concerns over use of the internet that includes, for example, the following:

- Internet searches for terms related to extremism
- Visits to extremist websites
- Use of social media to read or post extremist material
- Grooming of individuals

The Prevent Duty requires a school's monitoring and filtering systems to be fit for purpose.

Roles and Responsibilities

As eSafety is an important aspect of strategic leadership within the school, the Head and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored.

The named eSafety co-ordinator in our school is **Laura Hughes** who has been designated this role as a member of the senior leadership team. All members of the school community have been made aware of who holds this post. It is the role of the eSafety co-ordinator to keep abreast of current issues and guidance through organisations such as CWAC LA, CEOP (Child Exploitation and Online Protection) and Childnet.

Senior Management and Governors are updated by the Head or eSafety co-ordinator and all governors have an understanding of the issues and strategies at our school in relation to local and national guidelines and advice.

This policy, supported by the school's acceptable use agreements for staff, governors, visitors and pupils (appendices), is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: child protection, health and safety, home–school agreements, and behaviour/pupil discipline (including the anti-bullying) policy and PHSE.

eSafety skills development for staff

- Our staff receive regular information and training on eSafety issues in the form of regular staff training.
- Details of the ongoing staff training programme can be found in the School Development and Improvement Plan
- New staff receive information on the school's acceptable use policy as part of their induction.
- All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of eSafety and know what to do in the event of misuse of technology by any member of the school community
- All staff are encouraged to incorporate eSafety activities and awareness within their curriculum areas.

Managing the school eSafety messages

- We endeavour to embed eSafety messages across the curriculum whenever the internet and/or related technologies are used.
- The e-safety policy will be introduced to the pupils at the start of each school year.
- E-safety posters will be prominently displayed.
- E-safety messages are sent to parents via 'ParentMail', Twitter and Facebook

eSafety in the Curriculum

- Educating pupils on the dangers of technologies that maybe encountered outside school is done informally when opportunities arise and as part of the eSafety curriculum.
- E-safety awareness day is a focus each year in line with the UK safer internet centre and the internet safety day they promote
- Pupils are taught about copyright and respecting other people's information, images, etc through discussion, modelling and activities.
- Pupils are aware of the impact of online bullying and know how to seek help if they are affected by these issues. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/ carer, teacher/ trusted staff member, or an organisation such as Childline/CEOP report abuse button.
- Trips and visitors are planned for throughout the year to provide further opportunities for educating our young people about staying safe online and offline, such as police talks on internet safety, Crucial Crew, Safety Central
- E-safety messages are also delivered through the PSHE and RHE curriculum
- Purple Mash is a learning platform which is used across the school to deliver our computing curriculum and e-safety. Staying safe online is promoted within every unit of work and it provides an opportunity for children to try simulated email and blog tools in a safe environment
- At the start of each school year, pupils agree to the 'Acceptable Use Policy'.
- Parklands uses the tagline 'Zip it, Block it, Flag it' to support pupil' understanding of staying safe online.
- From EYFS to KS2, we progress from this basic whole school message to look at eSafety in more detail in Key Stage 2, in terms of appropriate '**Content, Contact and Conduct'.** As well as ensuring pupils are aware of their '**Digital Footprint'** and its impact and the '**Opportunity Cost'** of internet use and potential effect on wellbeing. (See attached document - Switched on Computing)

Passwords and Security

- Passwords should be changed regularly.
- Passwords must not be shared.
- Staff must always 'lock' the PC if they are going to leave it unattended (the picture mute or picture freeze option on a projector will allow an image to remain on the screen and also allow a PC to be 'locked').
- All users should be aware that the ICT system is filtered and monitored.
- All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's e-safety Policy.
- Pupils are not allowed to deliberately access on-line materials or files on the school network, of their peers, teachers or others.
- Staff are aware of their individual responsibilities to protect the security and confidentiality of school networks, SIMS MIS system.
- In our school, all ICT password policies are the responsibility of the Headteacher and all staff and pupils are expected to comply with the policies at all times.

Data Security

The accessing of school data is something that the school takes very seriously. Staff are aware of their responsibility when accessing school data. They must not;

- allow others to view the data
- edit the data unless specifically requested to do so by the Headteacher.

Managing the Internet

The internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people.

- Pupils will have supervised access to Internet resources through the school's fixed and mobile internet technology.
- Staff will preview any recommended sites before use.
- Raw image searches are only carried out by pupils under supervision.
- If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents will be advised to supervise any further research.
- All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources.
- All users must observe copyright of materials from electronic resources.
- You tube will be accessed by teachers only within a classroom situation.
- Teachers must search for and identify the appropriate clip before the children are asked to watch.
- Skype/zoom to be used only as a whole class activity lead by a member of staff.

Information system security

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection will be updated regularly.
- Security strategies will be discussed with LEA ICT Services

Managing filtering

- The school will work with LEA, DFE and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover an unsuitable site, it must be reported to the e-Safety Coordinator.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

INFRASTRUCTURE
System managed by LA remotely and onsite, also ICT-Co has access for blocking and unblocking with Head Teachers authorisation
ICT-Co can access and block site or sites at the time or LA/SBB can block instantly via Remote Access

- Staff and pupils are aware that school based email and internet activity can be monitored and explored further if required.
- The school does not allow pupils access to internet logs.
- The school uses management control tools for controlling and monitoring workstations.
- If staff or pupils discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the e-safety co-ordinator.
- It is the responsibility of the school, by delegation to LA ICT, to ensure that Anti-virus protection is installed and kept up-to-date on all school machines.
- Pupils and staff are not permitted to download programs or files on school based technologies without seeking prior permission from the computing lead and ICT support

Managing other technologies (social media/blogs/Youtube etc)

Social networking sites, if used responsibly both outside and within an educational context can provide easy to use, creative and free facilities. However it is important to recognise that there are issues regarding the appropriateness of some content, contact, culture and commercialism. To this end, we encourage our pupils to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.

- At present, the school endeavours to deny access to social networking sites to pupils within school. It is also noted that the age of the children would suggest that they are too young to sign up to social networking sites but may have access to them. Therefore all the advice and teaching is given in context of being SMART on line.
- All pupils are advised to be cautious about the information given by others on sites, for example users not being who they say they are.
- Pupils are taught to avoid placing images of themselves (or details within images that could give background details) on such sites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online.
- Pupils are always reminded to avoid giving out personal details on such sites which may identify them or where they are (full name, address, mobile/ home phone numbers, school details, IM/ email address, specific hobbies/ interests).
- Our pupils are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.
- Pupils are encouraged to be wary about publishing specific and detailed private thoughts online.
- Our pupils are asked to report any incidents of bullying to the school.
- Staff may only create blogs, wikis or other web 2 spaces in order to communicate with parents/pupils in line with school software choices eg Class Dojo/Google Classroom/Twitter

Mobile technologies

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Many existing mobile technologies such as gaming devices and Smart phones are familiar to children outside of school too. They often provide a collaborative, well-known device with possible internet access and thus open up risk and misuse associated with communication and internet use. Our school chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

Personal Mobile devices (including phones)

- The school allows staff to bring in personal mobile phones and devices for their own use. Only under exceptional circumstances does the school allow a member of staff to contact a pupil or parent/ carer using their personal device. For example, when a trip is outside of normal school hours/residentials.
- Pupils are not allowed to bring personal mobile devices/phones to school unless with the prior approval of the school. Those who do must hand them in to their teacher to be placed in a locked storage box. Pupil's phones must be password protected and switched off for the duration of the time they are in school.
- The school is not responsible for the loss, damage or theft of any personal mobile device.
- The sending of inappropriate text messages or emails between any member of the school community is not allowed.
- Permission must be sought before any image or sound recordings are made on these devices of any member of the school community.
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.
- Staff should not contact pupils outside normal school hours.

Use of Mobile Phones for Volunteers and Visitors

- When entering the building, there is a sign which states that mobile phones should be switched off.
- If they wish to make or take an emergency call they may use either the main or the manager's office. Neither are volunteers or visitors permitted to take photographs or recordings of the children without the Headteacher's permission.
- We believe that photographs validate children's experiences and achievements and are a valuable way of recording milestones in a child's life. Parental permission for the different ways in which we use photographs is gained as part of the initial registration at this school. We take a mixture of photos that reflect the pre-school environment; sometimes this will be when children are engrossed in an activity either on their own or with their peers. In order to safeguard children and adults and to maintain privacy, cameras are not to be taken into the toilets by adults or children. All adults whether teachers/practitioners or volunteers at the school understand the difference between appropriate and inappropriate sharing of images.
- All images are kept securely in compliance with the Data Protection Act.
- If a member of staff suspects that a mobile phone has been misused within the school then it should be confiscated but staff should not 'search' the

phone. The incident should be passed directly to SLT who will deal the matter in line with normal school procedures.

Managing email

The use of email within most schools is an essential means of communication for staff. In the context of school, email should not be considered private. We recognise that pupils need to understand how to style an email in relation to their age and good 'netiquette'.

- Staff have a school email account which should be used for school related emails and for planning.
- Any e-mails containing confidential information will be transferred only by the school's secured e-mail account.
- The senior leadership team and admin staff are responsible for the sending of emails through the secure account.
- It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary email histories can be traced. This should be the account that is used for all school business.
- Under no circumstances should staff contact pupils, parents or conduct any school business using personal email addresses.
- The school requires a standard disclaimer to be attached to all secure email correspondence, stating that, 'the views expressed are not necessarily those of the school or the LA'. The responsibility for adding this disclaimer lies with the account holder.
- E-mail sent to an external organisation should be written carefully before sending, in the same way as a letter written on school headed paper.
- Staff sending emails to external organisations are advised to cc. the Headteacher, line manager or designated account.
- The forwarding of chain letters this includes jokes and funny statements is not permitted in school.
- All e-mail users are expected to adhere to the generally accepted rules of network etiquette (netiquette) particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in e-mail communication, or arrange to meet anyone without specific permission
- Staff must inform the eSafety co-ordinator/ line manager if they receive an offensive e-mail.

Safe Use of Images - Taking of Images and Film

Digital images are easy to capture, reproduce and publish and, therefore, misused. We must remember that it is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness.

- With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment.
- If photos/videos are to be used online then names of pupils should not be linked to pupils.

- Staff must be fully aware of the consent form responses from parents when considering use of images. This is updated annually as part of the data collection exercise.
- Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, this includes when on field trips. However, with the express permission of the Headteacher, images can be taken provided they are transferred immediately and solely to the school's network and deleted from the staff device.
- Pupils are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of the others, this includes when on field trips.
- Photos taken by the school are subject to the Data Protection Act.
- Parents and carers are permitted to take photos/videos of their own children in school events. They are requested not to share photos/videos from school events on social networking sites if other pupils appear in the background.
- Parents attending school based events will be reminded of their responsibilities in relation to social media verbally and through notices.
- Photos for personal use such as those taken by parents/carers are not subject to the Data Protection Act.

Publishing pupil's images and work

On a child's entry to the school, all parents/guardians will be asked to give permission to use their child's work/photos in the following ways:

- on the school web site
- on the school blog
- on the school's social media accounts-Twitter/Facebook
- on the school's YouTube channel
- in the school prospectus and other printed publications that the school may produce for promotional purposes
- recorded/ transmitted on a video or webcam
- in display material that may be used in the school's communal areas
- in display material that may be used in external areas, ie exhibition promoting the school
- general media appearances, e.g. local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically)

This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue, e.g. divorce of parents, custody issues, etc.

Parents/ carers may withdraw permission, in writing, at any time. Pupils' names will not be published alongside their image and vice versa. E-mail and postal addresses of pupils will not be published. Pupils' full names will not be published.

Before posting student work on the Internet, a check needs to be made to ensure that permission has been given for work to be displayed.

Data storage

- Only encrypted USB pens are to be used in school.

Storage of Images

- Images/ films of children are stored on the school's network
- Pupils and staff are not permitted to use personal portable media for storage of images (e.g., USB sticks) without the express permission of the Headteacher
- Rights of access to this material are restricted to the teaching staff and pupils within the confines of the school network.
- Images are stored on the cloud and deleted when necessary.

Webcams and CCTV

- We do not use publicly accessible webcams in school.
- Webcams in school will only ever be used for specific learning purposes, i.e. monitoring hens' eggs and never using images of children or adults.
- Misuse of the webcam by any member of the school community will result in sanctions (as listed under the ' inappropriate materials' section of this document)
- Consent is sought from parents/carers and staff on joining the school, in the same way as for all images.
- CCTV is used on the school grounds for monitoring purposes.

Video Conferencing

- Permission is sought from parents and carers if their children are involved in video conferences
- Permission is sought from parents and carers if their children are involved in video conferences with end-points outside of the school.
- All pupils are supervised by a member of staff when video conferencing
- All pupils are supervised by a member of staff when video conferencing with end-points beyond the school.
- The school will keep a record of video conferences, including date, time and participants.
- Approval from the Headteacher is sought prior to all video conferences within school.
- The school conferencing equipment is not set to auto-answer and is only switched on for scheduled and approved conferences.
- No part of any video conference is recorded in any medium without the written consent of those taking part.

Use of Class Dojo for blended/remote learning and parent/teacher contact

- Teaching staff have access to Google Classrooms and Class Dojo
- This means of remote and blended learning must adhere to this policy and school expectations
- Communication with parents must be in line with school expectations as outline in appendix 5.
- Staff should, where possible, make contact with parents within working hours or use the schedule message option if working at a different, more convenient time (8:00 – 17:00)

- Work set should be appropriate and provide support such as examples or teacher modelled outcomes to support home learning

Use of Google Classrooms

G Suite for Education provides a set of education productivity tools used by educators around the world. It provides a secure learning platform for pupils to complete assignments and communicate with their teachers.

- Children use a Gmail login to access the school's Google Classroom
- Pupils must be taught about keeping their personal information private including their Gmail password.
- Google cloud contains the work completed by pupils
- Pupils can complete work in real time on Google Classroom both at home and in school.
- Google Classroom accounts are deleted within 4 weeks of a child leaving our school
- Pupils must agree to the AUP which includes information about Google Classroom.
- Communication with pupils must be in line with school expectations as outline in appendix 5.

Use of social media

- Teaching and admin staff have access to the school Twitter account, Instagram account and Facebook Page but must use it in accordance with the policy. (Social Media Policy)
- Images and videos uploaded onto the school's social media account must not name pupils and should only be of pupils whose parents have given consent.
- Staff must ensure that social media platforms are used solely for providing information to parents about school events or learning that has taken place.
- Pupils are not permitted to use social networking sites within school.
- Staff have access to the school's YouTube channel which is used by staff to share videos of learning and school trips.
- In the event of additional social media channels being used, the same etiquette applies.

Reporting

- All breaches of the e-safety policy need to be recorded using CPOMS. The details of the user, date and incident should be reported.
- Incidents which may lead to child protection issues need to be passed on to the teacher immediately – it is their responsibility to decide on appropriate action not the class teachers.
- Incidents that are of a concern under the Prevent duty should be referred to the designated lead immediately who should decide on the necessary actions regarding safeguarding and the Channel Panel.
- Incidents which are not child protection issues but may require intervention (e.g. cyberbullying) should be reported to the e-safety lead/SLT in the same day.

- Allegations involving staff should be reported to the Headteacher. If the allegation is one of abuse then it should be handled according to the DFE document titled 'Dealing with allegations of abuse against teachers and other staff'. If necessary, the local authority's LADO should be informed.
- Evidence of incidents must be preserved and retained whenever possible
- The curriculum will cover how pupils should report incidents (e.g. Ceop button, trusted adult, ChildLine).

Misuse and Infringements

Whenever a student infringes the e-Safety Policy, the final decision on the level of sanction will be at the discretion of the school management.

Inappropriate material

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the eSafety co-ordinator.
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the eSafety co-ordinator, depending on the seriousness of the offence; investigation by the Headteacher/LA, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences.
- Users are made aware of sanctions relating to the misuse or misconduct by formal interview and follow up letter from the Headteacher.

Equal Opportunities

Pupils with additional needs

The school endeavours to create a consistent message with parents for all pupils and this in turn should aid establishment and future development of the schools' eSafety rules. However, staffs are aware that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of eSafety issues.

Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of eSafety. Internet activities are planned and well managed for these children.

Parental Involvement

- A Digital Parenting' magazine by Vodafone is ordered and distributed to each family biannually.
- Parents/ carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to school as included in the home-school agreement.
- Parents/ carers are required to make a decision as to whether they consent to images of their child being taken/used in the public domain (e.g., on school website).

- The school disseminates information to parents relating to eSafety where appropriate in the form of;
  - Information and celebration evenings
  - Posters
  - Website
  - Blog posts
  - Twitter posts
  - Newsletter items

Review Procedure

There will be an on-going opportunity for staff to discuss with the eSafety coordinator any issue of eSafety that concerns them.

This policy will be reviewed annually and consideration given to the implications for future whole school development planning.

The policy will be amended if new technologies are adopted or Central Government change the orders or guidance in any way.

Appendix 1 – Acceptable use Policy Staff

Staff have signed the code of conduct which includes our school's acceptable use policy as shown below.

Acceptable use of technology

New technologies have become integral to the lives of children and young people in today's society, both within schools 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 internet access at all times.

This 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 ICT 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 IT in their everyday work.

The Trust will try to ensure that staff and volunteers will have good access to IT to enhance their work, to enhance learning opportunities for pupils' learning and will, in return, expect staff and volunteers to agree to be responsible users.

This policy covers all forms of communication, information retrieval (from any source), media and equipment, used for official business and regardless of origin, ownership or place of use, for example:

- email systems (internal and external)
- internet and intranet (email, web access and video conferencing including zoom, skype, teams and other conferencing materials)
- telephones (hard wired and mobile)
- computers – *this covers ANY computer used for work purposes, whether at the place of work or elsewhere*
- iPads and other tablet devices – *this covers ANY tablet device used for work purposes, whether at the place of work or elsewhere*
- photocopying, printing and reproduction equipment
- documents and publications (any type or format)

Acceptable Use Policy Agreement - all staff

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

For my professional and personal safety:

It is never acceptable to be 'friends' on Facebook with pupils (past or present). Staff members must inform the head teacher if they are 'Facebook friends' with any current school parents in school. This will only be permitted in exceptional cases. Staff may choose to be 'friends' or follow other staff on Social Media.
School staff's social media profiles should not be available to pupils or parents. If they have a personal profile on social media sites, they should not use their full name, as pupils may be able to find them.

- I understand that the school will monitor my use of the IT systems, email and other digital communications by using software within the school.
- I understand that the rules set out in this agreement also apply to use of school IT systems (e.g. laptops, email, websites etc.) out of school.
- I understand that the school IT systems are intended for educational use and that I will only use the systems for personal or recreational use within the policies (Online Safety, Safeguarding, Social Contact Outside School and IT Policy) 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 will immediately report any illegal, inappropriate or harmful material or incident I become aware of, to the appropriate senior member of staff within the school where I am based.

I will be professional in my communications and actions when using school IT 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 (including children on the school blog/twitter etc) I will do so with their parental permission and in accordance with the school's policy on the use of digital / video images. Where these images are published (e.g. on the school website) it

will not be possible to identify by name, or other personal information, those who are featured. I will not mention the school on social media in a negative or inappropriate manner.

- I will not use my personal equipment to record these images, unless I have explicit permission to do so (e.g. on a residential visit where it is not possible to use an ipad) and this will be agreed by the headteacher prior to making any recording. These will be deleted at the first available opportunity in the presence of the headteacher/agreed senior leader.
- I will not use social networking sites in school in accordance with the school's policies (Online Safety, Safeguarding, Social Contact Outside School and IT Policy).
- I will adhere to the school online safety, social contact outside school and safeguarding policies at all times.

I will only communicate with students / pupils and parents / carers using official school systems and email addresses. Any such communication will be professional in tone and manner. There will be no communication with parents/families using personal email addresses or telephones:

- No details of pupils will be stored on laptops or taken out of school unless on a visit/trip and they will be kept by the group leader confidentially.
- Photographs of children will not be taken on personal phones or cameras nor stored on laptops unless on a school residential and explicit permission has been given from the headteacher (as above). They must be deleted once transferred in school to the school IT system and this must be observed by a member of the SLT.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

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

- When I use my personal hand held / external devices (laptops / 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. Mobile phones will only be used in designated areas (by each school) during break/lunchtimes or with the consent of the Head teacher or a senior member of staff.
- I will not use personal email addresses on the IT systems when children are within the school building.
- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- I will ensure that my data is regularly backed up.
- 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.

- If I wish to install a programme onto equipment that is owned by school, I will contact the computing lead first to seek authorisation.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others. If equipment is damaged, I will report it to school immediately and be aware I may be responsible for the cost of repair if not covered by our school insurance.
- 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 policy to disclose such information to an appropriate authority.

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 school:

- I understand that this Acceptable Use Policy applies not only to my work and use of school IT equipment in school, but also applies to my use of school IT systems and equipment out of school and my use of personal equipment in school or in situations related to my employment by the school.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action which may include termination of contract. This could include a warning, a suspension, referral to Governors and / or 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 IT 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. I also confirm that all of my equipment is password protected and cannot be accessed without the password.

Appendix 2 – Acceptable Use Policies

Acceptable Use Policy for learners in KS1

I want to feel safe all the time.

I agree that I will:

- ask a teacher if I want to use the computers
- only open pages which my teacher has said are OK
- only work with people I know in real life
- tell my teacher if anything makes me feel scared or upset on the internet
- make sure all messages I send are polite
- show my teacher if I get a nasty message
- not reply to any nasty message or anything which makes me feel uncomfortable
- not give my mobile phone number to anyone who is not a friend in real life
- talk to my teacher before using anything on the internet
- not tell people about myself online (I will not tell them my name, anything about my home and family)
- not upload photographs of myself without asking a teacher

Anything I do on the computer may be seen by someone else and I know if I don't follow these rules, I might not be allowed to use a computer/iPad.

User Signature

Name
……
..

Date ……

Appendix 2 – Acceptable use Policy

.

Acceptable Use Policy for learners in Lower KS2

When I am using the computer or other technologies, I want to feel safe all the time.
I agree that I will:

- always keep my passwords a secret
- only visit sites which are appropriate for my learning purposes and have been directed by a teacher
- respect the school network and equipment
- show a responsible adult any content that makes me feel unsafe or uncomfortable
- keep the computer equipment on a flat surface
- follow school rules when using the equipment such as taking turns, passing iPads carefully
- not reply to any nasty message or anything which makes me feel uncomfortable
- discuss and agree my use of a social networking site with a responsible adult before joining
- always keep my personal details private. (my name, date of birth, family information, journey to school are all examples of personal details)
- always check with a responsible adult before I share images of myself or others
- never meet an online friend without taking a responsible adult that I know with me
- put equipment back gently and make sure the iPads go on charge
- only edit my own work
- if taking photographs, always ask others for their permission first (only take photographs if your teacher has allowed it)
- I will follow our school rules for being ready, respectful and safe online – ZIP IT, BLOCK IT, FLAG IT
- encourage others to follow the rules

I know that anything I share online may be monitored.
I know that once I share anything online it is completely out of my control and may be used by others in a way that I did not intend.
I know that if I don't follow these rules, I may not be allowed to use the school iPads/computers.

User Signature

Full Name .....

Date .....

Appendix 2 – Acceptable use Policy

Acceptable Use Policy for learners in Upper KS2

When I am using the computer or other technologies, I want to feel safe all the time.
I agree that I will:

- always keep my passwords a secret
- only visit sites which are appropriate for my learning purposes and have been directed by a teacher
- respect the school network and equipment
- when using Google Classroom make sure any messages sent to my teacher are appropriate and written in a formal style
- show a responsible adult any content that makes me feel unsafe or uncomfortable
- keep the computer equipment on a flat surface
- follow class rules when using the equipment such as taking turns, passing iPads carefully
- not reply to any nasty message or anything which makes me feel uncomfortable
- not use my own mobile device in school
- only give my mobile phone number to friends I know in real life and trust
- discuss and agree my use of a social networking site with a responsible adult before joining
- always follow the terms and conditions when using a site
- always keep my personal details private. (my name, family information, journey to school, are all examples of personal details)
- always check with a responsible adult before I share images of myself or others
- only create and share content that is legal
- never meet an online friend without taking a responsible adult that I know with me
- put equipment back gently and make sure the iPads go on charge
- only edit my own work
- if taking photographs, always ask others for their permission first (only take photographs if your teacher has allowed it)
- follow the SMART rules when using the internet. (safe, meeting, accepting, reliable, tell)
- encourage others to follow the rules

I am aware of the school rules for staying safe online ZIP IT, BLOCK IT, FLAG IT
I know that anything I share online may be monitored.
I know that once I share anything online it is completely out of my control and may be used by others in a way that I did not intend.
User Signature
I agree to follow this code of conduct and to support the safe use of ICT throughout the school
Full Name .....

Date .....

Appendix 3 – Parent letter – internet/e-mail use

Parklands Primary School

Parent / guardian name:……
Pupil name: ……
Pupil's registration class: ……

As the parent or legal guardian of the above pupil(s), I grant permission for my child(ren) to have access to use the Internet and other information computing technology (ICT) at school. I know that my daughter or son has signed a form to confirm that they will keep to the school's rules for responsible ICT use, outlined in the Acceptable Use Policy (AUP). I also understand that my son/daughter may be informed if the rules have to be changed during the year.

I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the Internet and mobile technologies, but I understand that the school will take every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials. These steps include using a filtered internet service, secure access to email, employing appropriate teaching practice and teaching e-safety skills to pupils.

I understand that the school can check my child's computer files, and the Internet sites they visit. I also know that the school may contact me if there are concerns about my son/daughter's e-safety or e-behaviour. I will support the school by promoting safe use of the Internet and digital technology at home and will inform the school if I have any concerns over my child's e-safety.

I am aware that the school permits parents/carers to take photographs and videos of their own children in school events and that the school requests that photos/videos are not shared on any social networking site such as Facebook if the photos/videos contain images of other children. I will support the school's approach to e-Safety and will not upload or add any pictures, video or text that could upset, offend or threaten the safety of any member of the school community

Parent / Guardians' signature:……

Your name (in block capitals): ……

Date:……

Appendix 4: Switched on Computing Guide to using the internet safely

Guide to using the internet safely

Introduction

As with any activity, using computers, and more particularly the internet, exposes children to a number of risks. Our responsibility is to minimise these risks, while still providing children with the educational benefits and value that the internet can bring. Tanya Byron's report, *Safer Children in a Digital World*, highlights three risks of the internet to children.

1. Inappropriate content
2. Inappropriate contact
3. Inappropriate conduct

It is also important to consider a child's digital footprint and the opportunity cost of the time he or she spends online. These issues are discussed in turn below.

Content

In schools, technical measures (such as filtering) are in place. This significantly reduces the risk of exposure to inappropriate content on the web. Many schools can edit their own filtering settings and some web-based services (e.g. Google) have 'safe' modes. Schools should ensure that filtering does not block educationally valuable content. Because technical solutions are rarely 100 per cent effective, many schools operate a policy of asking children to 'turn the screen off/turn the tablet over and tell an adult' if they inadvertently come across inappropriate content.

Contact

In addition to warning primary children of physical 'stranger danger', it is also important to ensure that the children's online activities within, and – more importantly – beyond school, do not endanger them through contact with people who would wish them harm. Excellent materials are available from Childnet International (www.childnet.com) and CEOP (www.thinkuknow.co.uk), among others, to educate children about the dangers of providing personal information online, and other risks.

Conduct

Children's behaviour online can result in harm to themselves or others. Teaching children from an early age to respect others' intellectual property, in part through modelling good practice, may make them less willing to make illegal copies of music, videos or software later in life. Remind children that they should observe the terms and conditions of any web sites they use, including those relating to age restrictions. Also ensure that your school's anti-bullying policy deals effectively with cyberbullying, so that any child who experiences it knows that they can report it, and that it will be taken seriously.

Digital footprint

Beyond the password protection of a school's learning platform, or similar commercial or local authority systems, content produced by children for the open web is likely to remain in one or more archives or indexes for an indefinite period of time. Similarly, logs of any user's online activities are maintained, usually securely, by website operators and service providers. While the opportunity to be visible to a wide audience for work is appealing, and has a lot to offer educationally, associating children's full names with work published on the internet creates a link between that and a child's online identity, which is unlikely to be appropriate for primary-level children.

Opportunity cost of being online

Time spent in front of a screen is time not being spent on other individual or social pursuits. *Switched on Computing* aims to link high-quality computing education with a diverse range of activities in the classroom and beyond. Children should be encouraged to see using technology as just one part of a broad, rounded experience of childhood.

Summary

As with any issue surrounding safeguarding children and young people, follow – and ensure the children in your care follow – your school's agreed policies, but also take any opportunities you can to emphasise to the children that, by and large, their behaviour online should mirror their (high) standards of behaviour offline. Ofsted's report, *The safe use of new technologies* (www.ofsted.gov.uk/resources/safe-use-of-new-technologies), makes a convincing case for educating children about online safety, rather than merely policing their access to content.

> 'Pupils were more vulnerable overall when schools used locked down systems because they were not given enough opportunities to learn how to assess and manage risk for themselves.'

You may find Ofsted's guidance on Inspecting Safeguarding a useful summary of requirements and expectations.

Educating children to make safe, responsible and effective use of the internet and other technologies is one of the aims of *Switched on Computing*.

Appendix 5: Remote/Blended learning

Class Dojo/Google Classrooms

Below outlines necessary measures to support home-school links while ensuring that blended learning can take place efficiently and effectively

Contact with parents/pupils:

- Contact via message should endeavour to be sent during working hours (8-6)
- Direct messages can and should be scheduled for a time during 8am and 6pm if working outside of these hours.
- Messages sent to parents must be formal and where a more challenging or sensitive question has been posed, staff should recommend a meeting or phone call to respond.
- Through Google Classroom, year 5 and 6 are able to send messages to their teachers/class staff. Pupils must be taught about using a formal style when asking questions or responding to a task.
- Staff must be cautious in all written communications as this can be open to interpretation and remains in the permanent written form.

Blended/Remote learning:

- Work for children who are isolating due to COVID-19 will be sent out via direct messages on Class Dojo (EYFS – Yr4) and Google Classroom (Y5-6).
- On the first day of absence, where it is not possible to send out work soon enough, parents should be guided towards the 'Home Learning' page on the school website for packs of work.

https://www.parklands.cheshire.sch.uk/home-learning/

- An English, maths and foundation piece of work will be the minimum daily expectation of work sent to parents for those children who are isolating.
- Work sent home must be: closely linked to the learning taking place in the classroom as possible; sequenced and of high quality; provide frequent and clear explanations of new content.
- Paper copies must be available for those who do not have access to computer software.
- Ideally, content will be sent out daily. Where necessary, work can be sent out for several days at a time.

Homework

- Homework (usually spellings to learn and times tables to practise) will be sent out electronically via Google Classroom or Class Dojo dependent on year group.

Appendix 6: e-Safety one page document for staff

Summary of the e-Safety policy

The named e-Safety co-ordinator in our school is **Laura Hughes**.

e-Safety in the Curriculum

- Educating pupils on e-Safety is taught regularly through the Computing, PSHE/RHE curriculum.
- E-safety awareness day is a focus each year
- Pupils are taught about respecting their own and other people's information, images, the impact of online bullying and know how to seek help if they are affected by it.
- E-safety trips and visitors are planned for throughout the year eg Safety Central
- Purple Mash is used to deliver our computing curriculum and e-safety. Staying safe online is promoted within every unit of work.
- Each year, pupils agree to the 'Acceptable Use Policy' and use the tagline '**Zip it, Block it, Flag it**' to support their understanding of staying safe online.
- Pupils will have supervised access to internet resources during lessons
- Staff will preview any recommended sites before use.
- Raw image searches are only carried out by pupils under supervision
- Pupils are always reminded to avoid giving out personal details on such sites which may identify them or where they are.

Personal Mobile devices/Managing Email

- Staff can bring in personal mobile phones and devices for their own use. Only under exceptional circumstances does the school allow a member of staff to contact a pupil or parent/ carer using their personal device. (The person making the call should endeavour to keep their number private by withholding their number.)
- Pupils who bring phones in must hand them to a teacher to be placed in a locked box.
- Staff have a school email account which should be used for school related emails.
- Any e-mails containing confidential information will be transferred only by the school's secured e-mail account
- Under no circumstances should staff contact pupils, parents or conduct any school business using personal email addresses.

Safe Use of Images -

- With the written consent of parents (on behalf of pupils), the school permits the appropriate taking of images by staff and pupils with school equipment.
- If photos/videos are to be used online, then names of pupils should not be used.
- Staff must be fully aware of the consent form responses from parents.
- Images/ films of children are stored on the school's network/shared drive
- Images and videos uploaded onto the twitter account must not name pupils and should only be of pupils whose parents have given consent.

Reporting

- All breaches of the e-safety policy need to be recorded using CPOMS. The details of the user, date and incident should be reported.

Passwords and Security

- Passwords must not be shared.
- Staff must always 'lock' the PC if they are going to leave it unattended

Prevent Duty

The prevent duty means that all staff have a duty to be vigilant and where necessary report concerns over use of the internet that includes, for example, the following:

- Internet searches for terms related to extremism
- Visits to extremist websites
- Use of social media to read or post extremist material
- Grooming of individuals

Appendix 7: **Current Legislation**

Keeping children safe in education 2020 – Annex C – online safety
The statutory guidance provides information on teaching online safety, faltering and monitoring, reviewing online safety and further information to support the school's teaching of e-Safety.

Acts relating to monitoring of email

Users of this list should note that legislation is open to change and should always verify that the references and versions given or linked are up to date before relying on them.

Data Protection Act 1998
The Act requires anyone who handles personal information to comply with important data protection principles when treating personal data relating to any living individual. The Act grants individuals rights of access to their personal data, compensation and prevention of processing.
http://www.hmso.gov.uk/acts/acts1998/19980029.htm

The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
http://www.hmso.gov.uk/si/si2000/20002699.htm

Regulation of Investigatory Powers Act 2000
Regulating the interception of communications and making it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998. The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, however, permit a degree of monitoring and record keeping, for example, to ensure communications are relevant to school activity or to investigate or detect unauthorised use of the network. Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored. Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation.
http://www.hmso.gov.uk/acts/acts2000/20000023.htm

Human Rights Act 1998
http://www.hmso.gov.uk/acts/acts1998/19980042.htm

Other Acts relating to eSafety

Racial and Religious Hatred Act 2006
It a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening.

Other laws already protect people from threats based on their race, nationality or ethnic background.

Sexual Offences Act 2003
The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. Schools should already have a copy of "*Children & Families: Safer from Sexual Crime*" document as part of their child protection packs.
For more information
www.teachernet.gov.uk

Communications Act 2003 (section 127)
Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

The Computer Misuse Act 1990 (sections 1 – 3)
Regardless of an individual's motivation, the Act makes it a criminal offence to gain:

- access to computer files or software without permission (for example using another persons password to access files)
- unauthorised access, as above, in order to commit a further criminal act (such as fraud)
- impair the operation of a computer or program

UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

Malicious Communications Act 1988 (section 1)
This legislation makes it a criminal offence to send an electronic message (e-mail) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.

Copyright, Design and Patents Act 1988
Copyright is the right to prevent others from copying or using work without permission. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer. Copyright infringement is to copy all or a substantial part of anyone's work without obtaining them author's permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else's material. It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.

Public Order Act 1986 (sections 17 – 29)
This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

Protection of Children Act 1978 (Section 1)
It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is a anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

Obscene Publications Act 1959 and 1964
Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Protection from Harassment Act 1997
A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.